

القرصنة الإلكترونية

أسلحة الحرب الحديثة

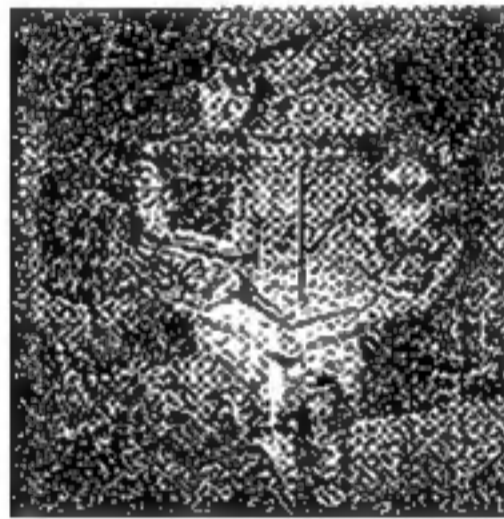


د. بشرى حسين الحمداني

القرصنة الإلكترونية

أسلحة

الحرب الحديثة



تأليف

الدكتورة بشرى حسين الحمداني

دار أسامة للنشر والتوزيع
عمان - الأردن

قبلاء ناشرون وموزعون
عمان - الأردن

الناشر

دار أسامة للنشر والتوزيع

الأردن - عمان

• هاتف : 5658252 - 5658253

• فاكس : 5658254

• العنوان : العبدلي - مقابل البنك العربي

ص.ب : 141781

Email: darosama@orange.jo

www.darosama.net

نبلاء ناشرون وموزعون

الأردن - عمان - العبدلي

حقوق الطبعة محفوظة

الطبعة الأولى

2014م

رقم الإيداع لدى دائرة المكتبة الوطنية
(2013 / 5 / 1687)

364.138

الحمداني، بشرى حسين

القرصنة الإلكترونية أسلحة الحروب الحديثة / بشرى حسين

الحمداني - عمان : دار أسامة للنشر والتوزيع ، 2013.

() ص .

ر ١ : (2013 / 5 / 1687)

الوصفات : / القرصنة / / الحروب الإلكترونية / / جرائم

الحرب /

ISBN: 978-9957-22-550-6

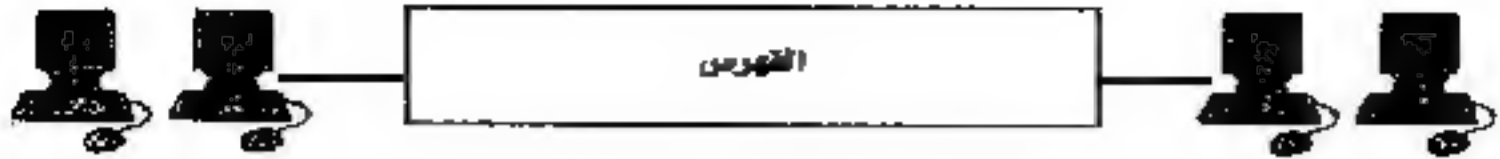


الفهرس

3	الفهرس
9	المقدمة

الفصل الأول

11	مدخل الى الهكرز (القرصنة الالكترونية)
12	مفهوم الهكرز أو التجسس
13	الاختراق
13	الفرق بين الهكرز والكرراكرز
14	الفرق بين الاختراق والهاكرز
14	اولاً - المخترق
15	ثانياً- الهاكرز
15	انواع الهاكرز
18	انواع القرصنة
20	بدايات القرصنة الالكترونية
20	تاريخ القرصنة
21	كيف يتم إختراق الأجهزة ؟
26	دروس جامعية في الهكرز
29	اساليب القرصنة
32	أكثر أساليب القرصنة شيوعاً
33	صفات القرصنة
34	للحماية من الهاكرز
37	كيف نقع ضحية الهكرز (القرصنة)
40	أشكال القرصنة
49	وسائل الارهاب الالكتروني



50	آثار الارهاب الالكتروني
51	الارهاب الالكتروني والقرصنة الالكترونية
52	سمات الإرهاب الالكتروني
54	هوامش الفصل الأول

الفصل الثاني

57	جرائم القرصنة الإلكترونية.....
59	المجرم الالكتروني (المعلوماتي)
59	الجريمة الإلكترونية
62	منفذي الجريمة الإلكترونية
62	أهداف الجرائم الإلكترونية
63	مراحل تطور الجرائم الالكترونية
69	اسباب جرائم القرصنة الالكترونية.
71	أنواع الجرائم الالكترونية
71	1 - الجرائم الاقتصادية
74	2- الجرائم الأخلاقية
75	3 - الجرائم الاجتماعية
79	4 - الجرائم الثقافية
84	5 - الجرائم السياسية
88	6 - الجرائم الجنسية
89	7 - الجريمة المادية Financial Crime
90	مكافحة جرائم الانترنت
94	هوامش الفصل الثاني

الفصل الثالث

97	حروب القرصنة الإلكترونية.....
98	الحرب الإلكترونية
101	تاريخ الحرب الالكترونية العالمية.



102	الحرب الإلكترونية في الحرب العالمية الأولى
104	الحرب الإلكترونية بين الحرب العالمية الأولى والثانية
105	الحرب الإلكترونية في الحرب العالمية الثانية
107	أسلحة الحرب الإلكترونية
109	الحرب الإلكترونية المستقبلية
113	الأهداف المعادية للحرب الإلكترونية
114	مجالات الحرب الإلكترونية
114	نماذج من حرب الفضاء الإلكتروني
116	نماذج من الحرب الدولية الإلكترونية
122	حروب القرصنة بين العرب والإسرائيليين
128	أساليب الحرب الإلكترونية
130	أحزاب القرصنة
131	حزب القرصنة العرب
133	هوامش الفصل الثالث

الفصل الرابع

135	الشبكات الاجتماعية وانتهاك الخصوصية
136	الشبكات الاجتماعية Social Network
138	البرمجيات الخبيثة على الشبكات الاجتماعية
139	أنواع الشبكات الاجتماعية
140	مميزات الشبكات الاجتماعية
141	نماذج من الشبكات الاجتماعية
143	الاستخدامات السلبية للشبكات الاجتماعية
147	المخاطر الأمنية في الشبكات الاجتماعية
152	مخاطر الخصوصية في الشبكات الاجتماعية
155	التقنيات الحديثة والخصوصية
161	القرصنة على الفيس بوك



163	مواقع التعارف... طريقة جديدة لاختراق الخصوصية
165	حماية خصوصية مستخدم الشبكات الإجتماعية
170	حمائق عن الخصوصية
172	هوامش الفصل الرابع

الفصل الخامس

175	القرصنة الإلكترونية في الدول العربية.....
176	الهاكرز العربي
179	المنطقة العربية سمن حرب القرصنة
181	أسباب زيادة القرصنة الوطن العربي.
185	الحماية الفكرية للبرامج
186	ترتيب الدول العربية في قرصنة البرمجيات العالمية.
188	الهاكرز العرب والمواقع الاسرائيلية
192	القرصنة الالكترونية في الاردن
194	السعودية والإمارات تصدران دول الخليج في الجرائم الالكترونية.
195	القرصنة الإلكترونية في الإمارات
197	القرصنة الإلكترونية في السعودية
200	القرصنة الالكترونية في الجزائر.
202	القرصنة في المغرب
203	القرصنة العراقية
204	القرصنة في الشرق الأوسط
206	هوامش الفصل الخامس

الفصل السادس

209	القرصنة الصحفية.....
211	ضحايا القرصنة الصحفية
212	قرصنة الصور



213	اسباب القرصنة الصحفية
213	اشكال القرصنة الصحفية
215	قرصنة مواقع صحفية الكترونية.
215	قرصنة شبكة الـ "CNN" الاخبارية
216	شركة حودادى الامريكية للقرصنة
217	المجلة المسيئة للرسول تتعرض للقرصنة الإلكترونية
218	مواقع الكترونية مغربية
219	صحيفة النهار اللبنانية
221	اختراق موقعي الجزيرة والعربية
221	اختراق موقع العربية.
222	اختراق موقع صحيفة، الوطن، السعودية.
223	المواقع الالكترونية الفلسطينية
225	وكالة انباء عراقية تفضح مؤسسات اعلامية عربية.
231	الملكية الفكرية
231	الحقوق الرقمية
233	انواع الملكية الفكرية.
234	براءة الاختراع
235	حق النشر.
237	هوامش الفصل السادس

الفصل السابع

239	التشريعات القانونية والقرصنة الإلكترونية.....
240	السويد
241	امريكا
242	بريطانيا
242	كندا
243	الدنمارك



243	فرنسا
244	هولندا
244	فنلندا
244	اليابان
244	المجر وبولندا
244	بلجيكا
245	قانون وقف القرصنة المعروف باسم SOPA
247	تشريعات حديثة في الجرائم الالكترونية
249	الحماية الفكرية في البلدان العربية
250	مصر
250	البحرين
250	العراق
250	السعودية
251	الإمارات
251	الأردن
251	لبنان
251	سوريا
252	الجزائر
252	القانون في انتظار الشكاوى والتبليغ
253	المغرب
254	حقوق النشر في عصر ثقافة الإنترنت
257	هوامش الفصل السابع
259	المصادر والمراجع



المقدمة

لم تعد الحرب في العصر الحديث عصر التكنولوجيا الحديثة تقتصر على الدبابات والقنابل والصواريخ . بل بات ما يعرف بالحرب الالكترونية حرب التكنولوجيا الحديثة بأسلحتها التقنية المتطورة . انه عصر الحرب المعلوماتية حرب الاختراقات والتجسس الالكتروني لأخطر المواقع وأكثرها حساسية ولم يقتصر الامر على الدول المتقدمة في مجال التكنولوجيا كامريكا وبعض دول اوربا . بل اضحت الدول العربية واحدة بل طرفاً أساسياً في حرب القرصنة الالكترونية وهو ما يحاول الكتاب تسليط الضوء عليه.

فمع التطور التكنولوجي المتزايد الذي نشهده، أصبحت تكنولوجيا التجسس حقيقة واقعية، ووصلت إلى مراحل متقدمة، فهبات بمقدورها التنصت أو تصوير أو تعقب أي فرد مستهدف بواسطة عدد من البرامج والأجهزة الإلكترونية والرقمية التي يفتتها، وإذا استمرت تكنولوجيا التجسس في التطور المتسارع وغير المنضبط، فقد تؤدي بالبشرية إلى القول: وداعاً للخصوصية

وانتشرت في الآونة الأخيرة المشرات من برامج التجسس التي تقوم بجمع المعلومات عن جهاز الكمبيوتر وعن الشخص وإظهار العديد من الإعلانات على النواهد المنبثقة.

فضلاً عن هذا كله إنتشرت الديدان التي تعجز أقوى البرامج المضادة للفيروسات عن ردها وتسبب العديد من الأضرار على جهاز الكمبيوتر، بالإضافة الى أحصنة طروادة Trojan والهاكرز (Hackers).

وقد تحول الفضاء الاعلامي و الشبكة العنكبوتية إلى ساحة حرب عقول و تقنيات و فييات و خبرات في المجال الالكتروني ولعل أكثر المجموعات فاعلية و نشاطاً التي عرفنا بها من الإعلام ومن الفضاء الافتراضي هي الهكرز أو التجسس التقني



وهذا البحث بشكل عام يُعبر تحريضاً على القرصنة الإلكترونية . بل لتوعية عما يدور من حولنا في هذا العالم الواسع ، ألا وهو عالم الإنترنت بعد اسقاط مصطلح الأمن الإلكتروني الذي كنا نَشْدُق به في يادى استقبالنا لهذا الصيف الغرب الذي بات يشاركنا حياتنا قبل ان يتحول الى جاموس لخصوصياتنا . ولم يعد العالم الافتراضي بمعزل عن السيطرة والأمن والاختراق ما دامت التكنولوجيا في تطور مستمر وما دام عقل الانسان لا يستطيع .

نستعرض خلال الكتاب عدداً من المواقع الإلكترونية في العالم كافة التي تعرضت وتعرض لكل يوم للقرصنة والاختراق بل نكاد نجزم بعدم وجود دولة في أي مكان في العالم ، سلمت من اعمال قرصنة . وتبقى سبل الدفاع والحماية هي ما يحول نجاح تلك الهجمات أو يجعلها لم تتم مهامها.

وبعيداً عن ساحات المعارك حيث دوي المدافع وانفجارات لقنابل وصوت الرصاص وتناثر الأشلاء وأساليب القتل البشعة ، تبدأ ساحات معارك أخرى لا تقل ضراوة عن مثيلتها العسكرية لكنها لا تخلف جثثاً وإن كانت تخلف دماراً وخسائر مادية ومعنوية ، إنها حروب النت .

تعاظم دور الحرب الإلكترونية لتشكل البعد الرابع بين أسلحة القتال البرية ، والبحرية ، والجوية والدفاع الجوي ، في التأثير بفاعلية على كفاءة هذه النظم الإلكترونية . لذلك سارعت دول العالم إلى تسليح مختلف أنواع قواتها بوسائل الحرب الإلكترونية.

واحتتم كلامي بالقول ان ما يقوم به بعض القراصنة من تحريب وسرقة للمعلومات ليس هو بالشئ البسيط ، اذا ما قورن باعمال قد تحدث اضراراً يمكن ان تؤدي الى نشوب حرب بين دول العالم.

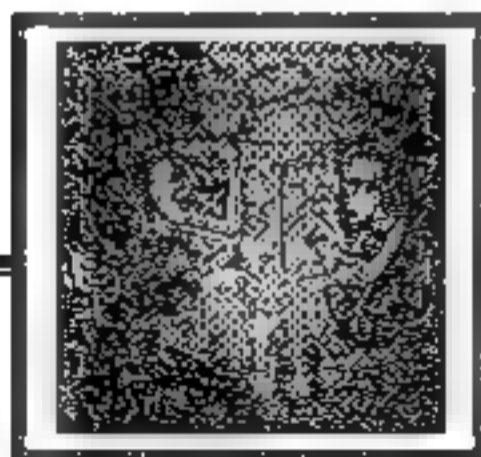
المؤلفة



الفصل الأول

مدخل إلى الهكرز

(القرصنة الالكترونية)





مفهوم الهكرز أو التجسس

نتيجة للتطور التقني والثورة الالكترونية التي الفت بظلالها على مناحي الحياة كافة، أصبحت شبكة الإنترنت ميداناً لصراعات من نوع جديد حملت كل أدوات التدمير الإلكتروني كالتجسس والاختراق وتدمير المواقع الإلكترونية الحكومية وغير الحكومية، والتحكم في تغيير قواعد بيانات قد تصل في خطورتها إلى تهديد الأمن القومي لبعض الدول، مما دفع بعض خبراء الإنترنت للاعتقاد أن الشبكة العنكبوتية أصبحت على حافة الانهيار.

بدأت كلمة hackers ككلمة تحمل معنى يختلف تماماً عما تحمله هذه الأيام، فقد بدأت كصفة تشير لعبقرية مبرمجي الكمبيوتر وقدرتهم على ابتكار أنظمة وبرامج حاسوب أكثر سرعة، ومن أشهر من اكتسب هذه الصفة (دينيس ريتش) و (كين تومسون) اللذان صمما برامج اليونكس عام 1969.

أما الهاكرز بالمفهوم السيئ فلم يكن لهم وجود قبل عام 1981، وهو عام ظهور أول حاسوب شخصي من إنتاج شركة IBM.

ذلك أن عملية القرصنة الإلكترونية كانت غاية في الصعوبة لعدة أسباب منها أن النسخ الأولى للحواسيب كانت ضخمة، وتحتاج إلى غرف كبيرة ذات درجات حرارة ثابتة، أما انتهاك خصوصية الآخرين فكانت تأخذ أشكلاً أخرى كالالتصص على هواتف الآخرين من خلال شركات الهواتف المحلية وتعتمد تداخل الخطوط لإصغاء المزيد من المرح والتسلية على الأمر، ناهيك عن التصص على أسرار المنتهكين وأحياناً ابتزازهم، وقد حدا ذلك بإحدى الشركات الأمريكية إلى فصل مجموعة الشباب العاملين فيها واستبدالهم بطاقم من الفتيات.

في بادئ الأمر عُرف قراصنة الكمبيوتر بالكرakers كوصف لمجموعة الأشرار الذين يلجأون إلى حواسيب الآخرين منتهكين خصوصيتهم، وكتمييز لهم عن الهاكرز وهم الأخيار، لكن مع مرور الزمن أصبح اللفظ يطلق على الفريقين دون تمييز وأصبحت العبارة بشيوع اللفظ لا بما كان يشير إليه.





عادة ما يعرف الهكر بأنه شخص غامض . يخترق كيف ما يشاء والناس تخاف منه . ويعتبر شخصية كبيرة ويكون له أعوان يلحقون حلف شهرته وقد يتلبسون بها في عصرنا الحالي انقلبت الموازين . أصبح الصغار كبارا بعقولهم في عالم الهكر أعمارهم تتراوح ما بين الـ 16 سنة و الـ 20 سنة . في هذا السن تجد كثيرين معترفين في عالم الهكرز . منهم الطيب ومنهم الخبيث . المخترقون أجناس . وقد تجد فيهم من يساعد الناس في استرجاع بياناتهم و بريدهم الإلكتروني . ومنهم من يقوم بسرقة الناس مدعيا أنه شخص طيب وهو في الأصل متلصص يريد أن يخترق عبثا . مكثرت عمليات الاختراقات في العالم العربي .

الاختراق

الاختراق بشكل عام هو القدرة على الوصول لهدف معين والدخول على الأجهزة بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بها بهدف التطفل على خصوصيات الآخرين والحق الصرر بهم .
ويطلق على المخترق مصطلح (Hacker) وحينما يتمكن المخترق من إحداث الأضرار كحذف ملفات أو تشغيل ملفات مؤذية أو وضع وزارعة ملفات تجسسية (أحصنة طروادة) أو فيروسات أو أي نوع من هذه الأنواع فهو مخرب (Cracker).

ويتم الاختراق عن طريق معرفة الثغرات الموجودة في النظام والتي غالباً ما تكون في المنافذ أو (Ports) الخاصة بالجهاز . ويمكن وصف هذه المنفذ بأنها بوابات للكمبيوتر على الشبكة العالمية تسمح لها بالدخول .

الفرق بين الهكرز والكراكرز

معنى كلمة كراكرز " Crackers " وهي الكلمة المرادفة لكلمة هكرز فالكراكرز هم الأشخاص الذين يقومون بالدخول إلى الأنظمة عنوة مستخدمين أساليبهم ومهاراتهم المبتنية على إكتشاف الأخطاء البرمجية التي يخلفها





الهاكرز ببرامجهم .. متبعين سياسة كسر الأكواد وسياسات تخريبية وقد يستعمل شتى الوسائل للوصول إلى هدفه وهو .. التخريب على الآخرين.

يوجد فرق كبير بين الهاكرز والكراكر . الهاكرز هم الذين بنوا الانترنت ، وهم الذين يتحكمون بإنشاء المواقع يعمل الكمبيوترات بكل شيء تراه على الانترنت أما الكراكر فهم الأوغاد من الذين لا هم لهم سوى إفساد و تخريب المواقع و سرقة البرامج و البحث عن الكراك لبرنامج أصلي و البحث عن أرقام الفيزا و أرقام الحسابات في البنوك والائتمالات الشخصية بالأفراد.

الهاكرز هم أشخاص أصلاً مبرمجين محترفين طوروا قدراتهم وأصبحوا يستطيعون التسلل إلى الأجهزة والمواقع وغيرها وأسمهم بالعربي مخترقون أو متسللون أما الانجليزي وهو الشائع الكتابة بنطقه بالعربي هو (HACKERS).

بعض الهاكرز يتعلمون هذا العلم للتكبر والمسطو على غيرهم فيسرق إيميلات أصحابه ويهدد غيره ويخترق أي موقع لا على التعيين فقط للشهرة وبعضهم يخترق أجهزة بنات لسحب صورهن والعياد بالله والتهديد بنشر الصور وهذا النوع يجب الإمساك به وسجنه لأنه يعتبر فساداً في الأرض وبعض الهاكرز المحترفين يخترقوا سيرفرات البنوك ويسحبوا منها فيزا و أموال لتحويلها وهو ما حدث قبل فترة ليست بالبعيدة.

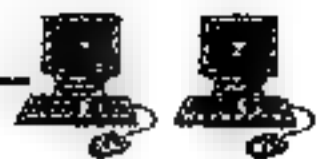
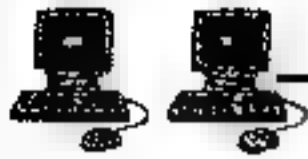
أذ قامت مجموعة من الهاكرز باختراق بنك معروف في السعودية فحولت ريال واحد من كل حساب وكان عدد الحسابات البنكية كثيرة قد تصل إلى 1000 حساب . فحولوا الأموال إلى حسابات الهاكرز لكي لا يشعروا أصحاب الحسابات من أن أموالهم قد سرقت وكثير من وسائل السرقة والتهديد والابتزاز.

الفرق بين الاختراق والهاكرز

أولاً - المخترق

المخترق: وهو شخص لا علم له بأي لغة من لغات البرمجة إنما تتم عمليات الاختراق التي يجربها عن طريق برامج إختراق موجودة بكثرة على الشبكة





مجانبة و المخترق والذي يسمى (بالكراكز) أو في علم الهاكرز بالمبتدي وهو شخص يجد برامج الهجوم وبطبيقاتها وهو غالباً لا يفقه طريقة استخدامها ولكن ينم استخدامها من جهته بعشوائية ولهذا فمن الممكن قيامه بدمار واسع أحياناً دون أن يدري بما فعله أساساً.

ثانياً- الهاكرز

هو شخص يستمتع بتعلم لغات البرمجة وأنظمة التشغيل وهو الذي يستمتع بالبرامج أكثر مما يشغلها ويحب أن يتعمق فيها ويتعلم المزيد عنها ويدقق في محتوياتها ويحاول إضافة أشياء فيها ويطورها وهو الذي يؤمن بوجود أشخاص آخرين يستطيعون القرصنة ومن هم أفضل منه ويوجد هكرز آخرين ويحاول أن يستفيد منهم ويفيدهم وبهذا ندرك إنه يصمم ويحلل البرامج وأنظمة التشغيل بسرعه وهو الشخص الخبير بلغة برمجة ما أو نظام تشغيل معين.

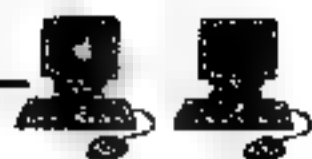
ولدية معلومات بخبايا أنظمة التشغيل والثغرات الموجودة فيه وهو ما يسمى (بالهاكر المحترف) ويكثر هؤلاء في أوروبا وأمريكا وقليل منهم في آسيا وخصوصاً في منطقة الشرق الأوسط والتي بدا يظهر الآن كثير منهم ولعل مايفعل الآن في المنتديات الفضائية.

انواع الهاكرز

يمكن تقسيم الهاكرز بمفهومه إلى الآتي:

- 1 - المحترفون: هم الفريق الأخطر لأنهم يعلمون ماذا يريدون وماذا يفعلون وكيفية الوصول إلى أهدافهم باستخدام ما لديهم من علم يطورونه باستمرار بالإضافة إلى استخدام البرامج الجاهزة المتطورة، إلا أنهم يعتمدون على خبرتهم في لغات البرمجة والتشغيل وتصميم وتحليل وتشغيل البرامج بسرعة، كما أن هوايتهم الأساسية معرفة كيفية عمل البرامج لا تشغيلها. إن أهداف هذا الفريق أكبر وأخطر من الفريق السابق، فأهدافهم المصارف وسحب الأموال من حساب العملاء، أو التلوج إلى أخطر المواقع وأكثرها حساسية والتلاعب ببياناتها أو





تدميرها ، ولم يعلم من شرهم أعتى سدة التكنولوجيا في المسالم
كميكروسوفت وياهو ووزارة الدفاع الأمريكية ووكالة ناسا ، والقائمة
طويلة ..

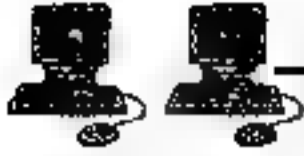
هم الذين يحملون درجات جامعية عليا تخصص كمبيوتر ومعلوماتية
ويعملون محلي نظم ومبرمجين ويكونوا على دراية ببرامج التشغيل ومعرفة عميقة
بخطاياها والثغرات الموجودة بها.

تنتشر هذه الفئة غالبا بأمريكا وأوروبا ولكن انتشارهم بدأ يظهر بالمنطقة
العربية وهذا لا يعني هذا أن كل من يحمل شهادة عليا بالبرمجة هو بأي حال من
الأحوال كراكر ولكنه متى ما اقتحم الأنظمة عنوة مستخدما أسلحته البرمجية
العلمية في ذلك فهو بطبيعة الحال أحد المحترفين.

2 - الهواة : يعتمد الهواة على برامج التجسس الجاهزة والمتاحة في كل مكان سواء
عن طريق الشراء أو التحميل عن شبكة الإنترنت ، ويقوم الهاكرز بزرع ملفات
التجسس patches & Trojans في حواسيب الضحايا عن طريق البريد
الإلكتروني أو ثغرات الوندوز التي يكتشفها البرنامج.

هذا الصنف من الهاكرز أهدافه طفولية حيث يسعى لإثبات نجاحه في
استخدام هذه البرامج وانضمامه إلى قائمة الهاكرز بهدف التفاخر بين الأصحاب
كشخص يمتلك مواهب يفتقدها بعضهم ، وهؤلاء ككل ما يشغلهم هو التسلل إلى
حواسيب الآخرين وسرقة بريدهم الإلكتروني والتلاعب في إعدادات هذه الأجهزة مع
ترك ما يفيد أنهم فعلوا ذلك كشكل من أشكال الغرور والتباهي بالنفس.

إما أن يكون أحدهم حاملا لدرجة علمية تسانده في الاطلاع على كتب
بلغات أخرى غير لغته كالأدب الإنجليزي أو لديه هواية قوية في تعلم البرمجة ونظم
التشغيل فيظل مستخدما للبرامج والتطبيقات الجاهزة ولكنه يطورها حسبما
تقتضيه حاجته ولربما يتمكن من كسر شيفرتها البرمجية ليتم نسخها وتوزيعها
بالمجان.



هذا الصنف ظهر كثيرا في العامين الأخيرين على مستوى المعمورة وساهم

في إنتشاره عاملا: -

الأول، إنتشار البرامج المساعدة وكثرتها وسهولة التعامل معها.

ثانيا إرتفاع اسعار برامج وتطبيقات الكمبيوتر الأصلية التي تنتجها الشركات مما

حفز الهواة على إيجاد سبل أخرى لشراء البرامج الأصلية بأسعار تقل كثيرا

عما وضع ثمنها لها من قبل الشركات المنتجة

3 - الهكر الاخلاقي: هو شخص يمتلك القدرة على الاختراق والحماية من

الاختراق يمتلك احدي الشهادات المخصصة لممارس طبيعة عمله كهاكر

اخلاقي، كما يسخر تلك الفنون "الاختراق والقرصنة" لخدمة المجتمع إما بتقديم

خدمات أمنية احترافية أو باكتشاف الثغرات في تطبيقات وأنظمة دولية وإشعار

الشركات المتضررة بخطورة تلك الثغرات، ولكن لا يتم كل ذلك إلا بعد توقيع

اتفاقية وتخطيط مسبق مع الجهة المراد اختبارها، أي أنه لا يجوز له الدخول لأي

مكان واختراقه "بحجة" فحصه ! يجب ان يأخذ الموافقة اللازمة لذلك قبل أي

خطوة متبعة.

وللهالك الاخلاقي شروط وأحكام يجب عليه اتباعها والموافقة عليها

بالتوقيع على اتفاقية تسمى Code Of Ethic وهي اتفاقية أخلاقية تهدف إلى أن

الهاكر الأخلاقي يجب أن يحافظ على السرية التامة في أي اختبار اختراق ولا يقوم

بتسريب أي معلومات عن الجهة المستهدفة أو الثغرات المكتشفة وعلى أن يقوم بتقديم

تقرير كامل يوضح فيه جميع الثغرات الأمنية والحلول مما يساعد الجهة المعنية

باختبار تأمين مصادرها من المخترقين، كما أن أي إخلال بأحد نصوص الوثيقة

الأخلاقية قد يعرض الهاكر الأخلاقي للمطالبة القانونية والمحاكمة أمام الجهات

المختصة.

ما المستقبل الوظيفي لهذا الشخص فيمكن للجهات استخدام الهاكر

الأخلاقي في كثير من الجوانب المتعلقة بأمور الاختراق وعمليات الهاكرز وعلى

سبيل المثال لا الحصر، اختبار تطبيقات الويب والمواقع على الانترنت وكشف



الثغرات الأمنية، واختبار الشبكات السلكية واللاسلكية وكشف نقاط الضعف فيها، وعمل تدقيق أمني للتطبيقات الداخلية والخارجية. أنه يمكننا استخدام الهاكر الأخلاقي لأي تقييم أمني هدفه كشف العيوب الأمنية قبل استغلالها من قبل المخترقين أو الأشخاص الذين يبحثون عن كشف معلومات سرية. هو الذي يحمي وفي المقابل يأخذ مقابل ماديًا.

4 - والهكر اللااخلاقي هو الذي يدمر ولا يتخذ شيئاً وقد يقبض عليه ويوضع في السجن لمجرد الهواية.

أنواع القراصنة

هناك أنواع مختلفة من "المهاجمين" القراصنة والذين يتم تصنيفهم تبعاً لدوافعهم أو حسب مجال خبراتهم :

1- القرصان الأبيض القبة (White hat hacker) أو ما يُعرف أيضاً باسم القرصان الأخلاقي هو مصطلح يُطلق في عالم تقنية المعلومات على شخص تعارض قيمه انتهاك أنظمة الحواسيب الأخرى. يركز القرصان ذو القبة البيضاء على حماية الأنظمة، على عكس القرصان ذو القبة السوداء الذي يحاول اختراقها.

والقرصان الأبيض يمارس ما يعرف بـ«القرصنة الأخلاقية» هو مصطلح يُطلق في عالم تقنية المعلومات على شخص تعارض قيمه انتهاك أنظمة الحواسيب الأخرى. ويركز القرصان ذو القبة البيضاء على حماية الأنظمة، على عكس القرصان ذو القبة السوداء الذي يحاول اختراقها.

وتعريف آخر، القرصان ذو القبة البيضاء هو شخص مصرّح له باستخدام الوسائل الممنوعة لمعالجة أخطار أمن الحواسيب والشبكات.

وتعريف آخر، القرصان ذو القبة البيضاء هو شخص مصرّح له باستخدام الوسائل الممنوعة لمعالجة أخطار أمن الحواسيب والشبكات.



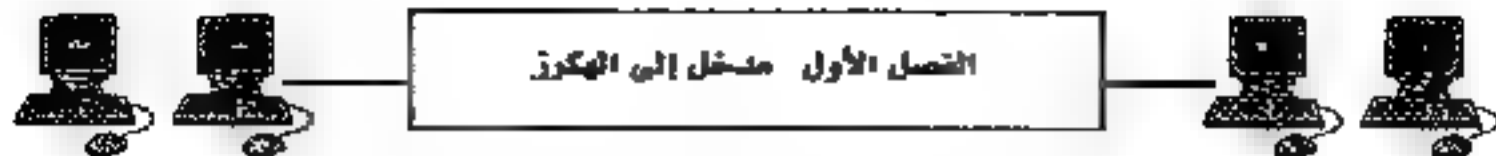


2- الهكرز ذو القبعة السوداء هو الشرير أو الرجل السيئ. خصيصاً في أفلام الغرب الأمريكي (Western) مثل هذه الشخصية التي ترتدي قبعة سوداء على النقيض من الأبطال ذوي القبعة البيضاء وغالباً ما تُستخدم هذه العبارة مجازياً في الحوسبة حيث تعود إلى المخترق الذي يقتحم الشبكات أو الحواسيب أو يصنع فيروسات الحاسوب للتخريب أو الحصول على المال.

3- الهكرز ذو القبعة الرمادية (Grey hat hacker) القرصان رمادي القبعة هو مصطلح يُطلق في مجتمع أمن الحواسيب على القرصان الذي يقوم بأعمال قانونية أحياناً، أو بمساعدة أمنية كما يعمل عليه ضميره أحياناً، أو باحتراق موز في أحيان أخرى.

إنه باختصار عبارة عن مريج من القرصان ذي القبعة البيضاء و القرصان أسود القبعة، لذا اختير له اللون الرمادي كلون وسط بين الأبيض والأسود. في العادة، لا يقوم هذا النوع من القراصنة بالاختراق لأغراض خبيثة أو لمصلحة شخصية، بل لزيادة خبرته في الاختراق واكتشاف الثغرات الأمنية. إن أي اختراق يقوم به أحد هؤلاء تكون نتائجه مكلفة فيكفي أن نعرف أن تسلسل أحد هؤلاء لأحد أنظمة الكمبيوتر الحكومية لمدة نصف ساعة يستدعي على أقل تقدير 24 ساعة من العمل المتواصل من أحد خبراء الكمبيوتر لاكتشاف ماذا فعل ذلك المتسلل، وسد الثغرات التي نفذ منها وإصلاح الأعطاب التي أحدثها . أما الخسائر المادية فحدث ولا حرج، ويكفيها نموذجاً ما أحدثه روبرت موريس أحد مشاهير الهاكرز عام 1988 حين قام بتطوير أفعى اليونكس مما تسبب في تعطيل حوالي 6000 جهاز حاسوب وهو ما يوازي عُشر أجهزة الإنترنت في ذلك الوقت، وقدرت الخسائر المادية حينها ما بين 15 إلى 100 مليون دولار . وعلى الرغم من التفاوت الكبير بين الرقمين إلا أن الخسارة المادية فادحة مقابل لا شيء سوى رغبة عارمة لإثبات الذات بطريقة تضر بالآخرين وتقود إلى السحن في نهاية المطاف .





بدايات القرصنة الالكترونية

تم الاتفاق على مصطلح القرصنة الرقمية أو "الهاكينغ" في معهد ماساتشوستس للتكنولوجيا في الخمسينات من القرن الماضي، حيث كان يوحد ناد لنماذج من القطارات. وكان الطلبة يقضون أوقات فراغهم في استعمال الكمبيوتر، الذي كان مخترعا حديثا في ذلك الوقت. وقد كانت لهذه النماذج من القطارات (وخاصة النموذج IBM704) حواسيب كبيرة، لم يكن يسمح باستعمالها إلا للأشخاص المدربين بشكل جيد.

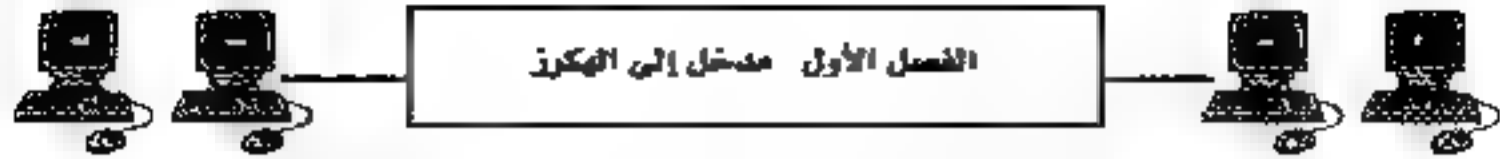
وقد كان قنوي هذه القطارات يقضون الليل للقيام بتجاربهم، حيث كانوا يكتشفون نفقات جديدة، ويقلبون الأزرار، باختصار كانوا يجربون كل التقنيات. هذا يعني أن هؤلاء الـ "هاكرز" كانوا يودون فقط اللعب واكتشاف حدود الممكن والقيام بتجارب واختبارات.

وحدثهم "الكراكر" هم من يقومون بأعمال تخريبية، والكراكر هو المصطلح الذي يطلق على القرصنة الرقميين الذين يقومون بأعمال تخريبية وغير مشروعة، كالتجسس وإلحاق الأضرار ببعض المصالح.

في جامعة دارمشتات التقنية، يتم تلقين الطلبة على طرق الهكرز لكن هذه المعرفة تنقل إلى الطلبة لأهداف جيدة. الدكتور مارتن ميك هو الذي يشرف على دراسة أساليب "الكراكر"، حيث يقوم الطلبة في إطار شبكة ضيقة بممارسة عمل "الكراكر" كفك الشفرات أو اختراق الأنظمة الالكترونية.

تاريخ القرصنة

ارتبط ظهور القرصنة واختراق رموز أنظمة الحاسوب مع ظهور أول الحواسيب الإلكترونية إلا أن تاريخ القرصنة واختراق رموز أنظمة الحاسوب يشمل الهجوم السيئ الذكر على شبكات الحاسوب من قبل مخترقي نظم الحاسوب



ومنتهكي القوانين ، كما يبين التقدم في مجال سرية المعلومات التي تعطي الإنترنت بالإضافة إلى تكنولوجيات أخرى كالاتصالات.

كما يرتبط تاريخ قرصنة الحاسوب مع الأحداث التي غيرت النظرة إلى سرية المعلومات كما نراها اليوم.

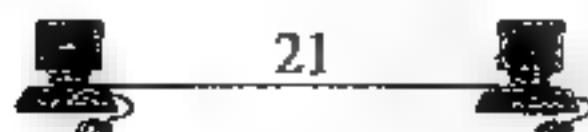
في عام 1971 اكتشف جون تـ درايبـر (الذي سمي بكابتـن كـرانـش)، بالتعاون مع صديقه جو انقرسيا ، وجود لعبة وهي عبارة عن صفاة توضع هدية داخل حبوب كـكابتن كـرانـش يمكن تعديلها لترسل نقمة بتردد حوالي 2600 هيرتز وهي تعادل نفس تردد المستعمل من قبل خطوط الاتصالات الخارجية AT&T لتدل على وجود خط رئيسي يسهل اختراقه فيمكن إرسال مكالمات خارجية عبره.

يمكن من خلال قطع الاتصال في طرف واحد من الخط ان يسمح للطرف الآخر من الخط إرسال المكالمات. وبعد احراء التجارب على استخدام الصفاة فكر في إنشاء (علب زرقاء) التي عبارة عن أجهزة إلكترونية قادرة على إرسال نفقات مختلفة مستخدمة من قبل شركة الهاتف وقد صدر الحكم عليه بعد توقيعه في اكتوبر من عام 1971 بمنعه عن العمل لمدة خمس سنوات بتهمة سرقة خدمة الخطوط الهاتفية بعدما توالى أحداث القرصنة الإلكترونية.

كيف يتم اختراق الأجهزة ؟

يعتمد إختراق الأجهزة على ملف يسمى الـ Server أو الـ Patch وان هذا الملف يمر بعدة مراحل وهي . تكوين السيرفر، فك ضغط السيرفر، تشفير السيرفر. ضغط السيرفر، دمج السيرفر، إرسال السيرفر إلى الضحية. كما أن هناك عدة طرق لتكوين السيرفر وعدة أساليب تستعمل لتلقي تبليغه وما اعنيه بالتبليغ: هو عبارة عن معلومات حاسوب الضحية التي تصل إلى المخترق بعد إرساله ملف السيرفر إليه. .. والشكل العام للتبليغ يحتوي على المعلومات التالية :-

▪ Victim State: OnLine حالة الضحية. متصل





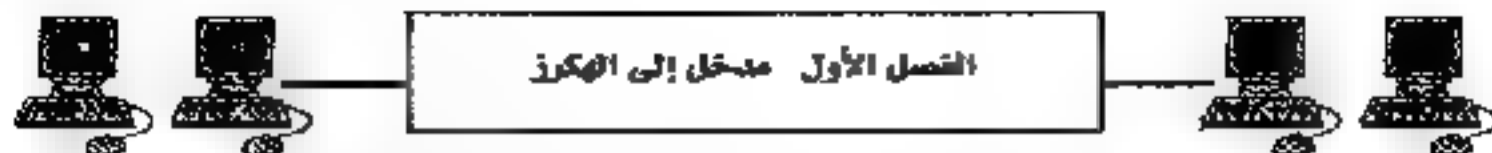
- Victim Name: Aseer إسم الضحية.
- IP: 106.156.689.68 البروتوكول .
- Server Size: 437 KB حجم السيرفر.
- Server Password: 123132 كلمة سر فتح السيرفر .

ويوجد هناك عدة أنواع من التبليغ أهمها :-

- 1 - التبليغ عن طريق البريد الإلكتروني :- وهذه الطريقة من التبليغ يقوم باستعمالها الفئة المبتدئة من المخترقين فتسبب نجاح وصول التبليغ هي 50% فقط وذلك بسبب وجود جدران حماية في شركات البريد الإلكتروني من أمثال Yahoo ، Hotmail ، Gmail ويعتبر أفضل هذه الشركات هو البريد التابع لشركة Google لأنه غير مجاني فتستطيع عدم تفعيل الجدار الناري فيه.
- 2 - التبليغ عن طريق صفحة CGI :- وهي عبارة عن صفحة يقوم بإنشائها المخترق ليصله تبليغ السيرفر الذي أرسله للضحية، ومن مميزات هذا النوع من التبليغ، السرعة وضمان وصول التبليغ بنسبة 70%، ويعتبر مستعملو هذا النوع من التبليغ من أصحاب المراحل المتقدمة في هذا المجال.
- 3 - التبليغ عن طريق موقع No-IP.COM :- ويعتبر هذا النوع من أنواع التبليغ الأخطر والأقوى، إذ أنه يضمن وصول التبليغ بنسبة 100% دون حدوث أية مشاكل وبسرعة عالية جداً، والفرق بين هذا التبليغ ومقية أنواع التبليغ أن هذا الموقع بعد عمل حساب شخصي لك به يقوم بإعطائك رقم IP ثابت دون أن يحدث تغيير بالرقم وخصوصاً لمستخدمي الـ Dial-UP، ويعتبر مستخدمو هذا النوع من التبليغ من أخطر الأشخاص وأكثرهم خبرة.

بعد فتح السيرفر في جهاز الضحية تحدث عملية فتح للمنفذ PORT الذي يستعمله البرنامج حيث أن لكل برنامج منفذ خاص فيه ولتأخذ مثلاً برنامج الـ ProRat الشهير الذي يستعمل المنفذ رقم 80، وبعد فتح المنفذ يقوم السيرفر بنسخ نفسه تلقائياً في منطقة بدأ التشغيل " Start Up "، وكما يقوم أيضاً بوضع نسخة





من نفسه في مجلد حساس من مجلدات الـ Windows وهو مجلد الـ System32 والهدف من هذه العملية ضمان بقاء الضحية على اتصال مع المخترق وضمان بقاء ما يسمى الـ Back Door أو كما يسميه البعض الإتصال العكسي أو خط الرجعة، وبالطبع تحدث هذه العملية في أجزاء من الثانية بحيث أن الضحية لا تشعر بأن هناك خلل أو اختراق قد حدث بالحاسب.

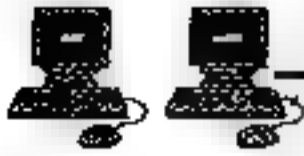
وبعد ذلك تحدث هناك عملية وصول التبليغ إلى المخترق وعملية إتصال المخترق بجهاز الضحية أو كمصطلح متداول عملية Connect مع الضحية.. وهكذا أصبح جهاز الضحية في متناول المخترق ولم يبق عليه سوى استلام المعلومات وإستغلالها والتمتع بتخريب خصوصياته.

وبهذا التفصيل لعملية وصول السيرفر أصبحنا ندرك ما هي الآلية المتبعة للاختراق وكيفية وصول المعلومات بطرق التبليغ الثلاث.

العمليات التي يمر بها السيرفر منذ لحظة تكوينه حتى لحظة إرساله :-
أولاً: تكوين السيرفر :- وهي عملية إنشاء سيرفر الاختراق وتحديد طريقة التبليغ التي يريد استخدامها المخترق وتحديد أيقونة السيرفر ورقم الـ IP وكلمة سر فتح السيرفر وقد نظرنا إلى هذا الموضوع في صفحات سابقة.

ثانياً: فك ضغط السيرفر :- وهي عملية يقوم بها المخترق بتحليل السيرفر إلى أجزاء ليسهل عليه تعديل بعض المعلومات، وليسهل عليه تشفيره وذلك يكون بإستخدام برامج خاصة لهذه العملية.

ثالثاً: تشفير السيرفر :- ونعني هنا بتشفير السيرفر أي أننا سوف نقوم بتغيير قيم الـ Hex الخاصة به حتى لا تستطيع الجدران النارية وأنظمة الحماية من اكتشاف السيرفر وتعطيل عمله عند استلامه من قبل الضحية. أمثلاً نريد تشفير سيرفر البرورات فنقوم بفك ضغطه وفتحه عن طريق برنامج تحرير قيم الـ هيكس Hex WorkShop وتعديل إحدى السطور الموجودة في هذا السيرفر، وطبعاً هناك سطور معينة هي التي يتم نظام الحماية كشفها أثناء عملية البحث. أمثلاً نأخذ السطر التالي "وهو سطر خاص لبرنامج الكاسبرسكاى الشهير بقوته



بحماية الأجهزة من المخترقين " AF0000 ونقوم بتعديله فيصبح كالتالي CA0001 ونقوم بحفظ العمل وإعادة ضغط السيرفر، فيصبح السيرفر غير مكشوف من قبل برنامج الحماية الكاسيرسكاى، وهكذا حتى نقوم بتشغيله عن جميع أنظمة الحماية.

رابعاً: إعادة ضغط السيرفر :- وهي عملية تجميع أجزاء السيرفر مرة أخرى بعد أن نقوم بتجزئته وفك ضغطه وذلك ليكون هناك ملف واحد فقط وذلك يسهل على المخترق إرساله إلى ضحيته دون إثارة أي شكوك.

خامساً: دمج السيرفر :- وهذه مرحلة مهمة جداً إذ تبعد الشكوك بنسبة 70٪ فالكثير من الناس لا يقبلوا استقبال أي شيء من ناس غرباء ويكون امتداده exe وهو الامتداد المتداول في سيرفرات الاختراق كغيره من البرامج التنفيذية التي تنتهي بهذا الامتداد، فيقوم المخترق الذكي بدمج السيرفر في صوره أو في ملف موسيقي.

سادساً: إرسال السيرفر إلى الضحية :- وتكون هذه هي العملية الأخيرة بدورة حياة السيرفر حيث يقوم المخترق بإرساله إلى ضحيته ليتم عملية الاختراق بشكل ناجح وسلس ومن الطرق المتداولة لإرسال السيرفر :-

• عن طريق المsnجر.

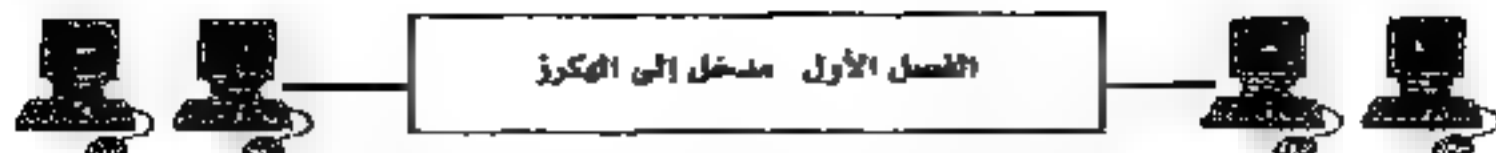
• عن طريق البريد الإلكتروني كملف مرفق.

• عن طريق وصلة ملفومة في المنتديات.

• عن طريق مواقع المحادثة.

ويتطلب إرسال السيرفر وجعل الضحية تقوم بفتحه يتطلب مهارة وقوة اقتناع من قبل المخترق كأن يكون اسم السيرفر وأيقونته مغريان بعض الشيء، أو أن يرسل إلى الضحية بريد إلكتروني من إيميل فتاة ويرفق معها صوره بحجة أنها فتاة تريد التعرف به وها هي صورتها ليشاهدما. وهناك الكثير الكثير من الطرق والابتكارات





بعض الطرق الأخرى المتبعة في اختراق الأجهزة :-

- 1 - الاختراق عن طريق الاتصال العكسي.
- 2 - الاختراق عن طريق المتصفح Internet Explorer.
- 3 - الاختراق عن طريق برنامج مشغل الملفات الموسيقية Real Player
- 4 - الاختراق العشوائي.

والكثير الكثير من الطرق التي تعتمد على ثغرات أمنية في نظام الـ Windows.

الوسائل المساعدة على اختراق جهازك ؟

1 - وجود ملف باتش أو تروجان

لا يستطيع الهاكر الدخول إلى جهازك إلا مع وجود ملف يسمى (patch) أو (trojan) في جهازك وهذه الملفات هي التي يستطيع الهاكر بواسطتها الدخول إلى جهازك الشخصي حيث يستخدم الهاكر أحد برامج التجسس التي ترتبط مع ملف الباتش الذي يعمل (ريسيفر) يستطيع أن يضع له الهاكر (اسم مستخدم) و (رمز سري) تخوله أن يكون هو الشخص الوحيد الذي يستطيع الدخول إلى جهازك وكذلك يستطيع أن يجعل جهازك مفتوحاً فيستطيع أي هاكر أن يدخل إلى جهازك !!

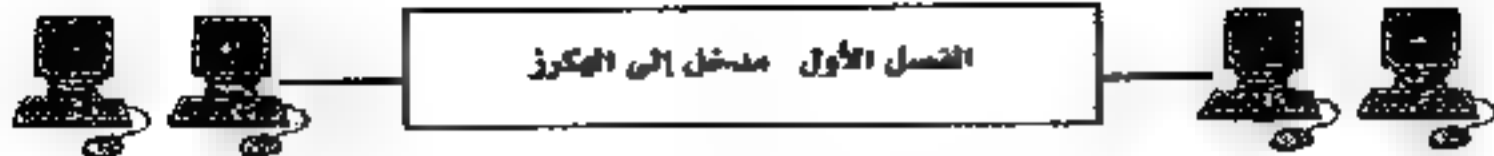
2 - الاتصال بشبكة الإنترنت

لا يستطيع الهاكر أن يدخل إلى جهازك إلا إذا كنت متصلاً بشبكة الإنترنت أما إذا كان جهازك غير متصل بشبكة الإنترنت أو أي شبكة أخرى فمن المستحيل أن يدخل أحد إلى جهازك سواء كان !!

ولذلك إذا أحسست بوجود هاكر في جهازك فصارع إلى قطع الاتصال بخط الإنترنت بسرعة حتى تمنع الهاكر من مواصلة العبث والتلصص في جهازك

3 - برنامج التجسس

حتى يتمكن الهاكر العادي من اختراق جهازك لابد أن يتوافر معه برنامج يساعد على الاختراق !



ومن أشهر برامج الهاكرز هذه البرامج:

Web Cracker 4

Net Buster

NetBus Haxporg

Net Bus 1.7

Girl Friend

BusScong

BO Client and Server

***** Utility

دروس جامعية في الهاكرز

من أهم الدروس التي يتلقاها الطلبة في تعليم الهاكرز هو أن يمتلك مجرمو الانترنت حيلة وفنونا متقدمة، ولذلك ينبغي على الطلبة أن يتلقوا تدريباً جيداً وأن يعرفوا كل الحيل، وكيف يمكن للمرء مواجهة هذه الهجمات الالكترونية وكذا تعلم فن الهجوم وفن الدفاع.

وليست جامعة دارمشتات التقنية وحدها من يقدم هذه الدروس وإنما يستطيع الطلبة تعلم هذه التقنيات أيضاً في كل من جامعة بوخوم وجامعة آخن، وكذلك المعهد العالي لمدينة بون- راين- زيغ و معهد ريفينسبورغ العالي والمعهد العالي لمدينة غيلسنكيرشن

لكن لا أحد يستطيع أن يمنع الطلبة من استخدام معرفتهم في أعمال غير مشروعة، وفي المعهد العالي لمدينة غيلسينكيرشن يلزم الطلبة بالتوقيع على التزام الشكتم عن المعرفة التي يتلقونها. رغم ذلك لا ينتظر الدكتور مارتن مينك الكثير من التوقيع على هذا الالتزام، بالنسبة إليه الضمير الأخلاقي للطلبة هو الذي يلعب دوراً كبيراً. ولحد الآن لم تسجل أية تجارب سلبية.

يقول الدكتور هاردموت بوول، الذي يُدرس في المعهد العالي بون- راين-

ربع، يقوم الطلبة عن طريق السهو باختراق عنوان الكتروني، وهذا أمر يمكن أن



يحدث. الشيء الوحيد الذي أطالب به هو الوضوح التام. أي ينبغي للطلبة أن يعتذروا و أن أقوم أنا بدوري بالاتصال بشكل فوري بالمؤسسة التي تعرضت لذلك

ينص الميثاق الأخلاقي لهذه الجمعية على صفحتها الخاصة على شبكة الانترنت على ان مبدأ حركة الهاكرز العالمية: "ينبغي أن يتم تداول المعلومات بحرية، فمن جهة ينبغي استعمال المعلومات العامة ومن جهة أخرى ينبغي حماية المعلومات الشخصية".

لكن كيف يمكن التعامل مع الهاكرز الذين يتمصون دور "روبن هود" - السارق الطيب الذي يسرق من أجل الفقراء - عندما يقومون بإغلاق بعض المواقع الالكترونية وتعطيلها من أجل "أعمال خيرية" كالتعبير عن احتجاج سياسي مثلا. ورغم أن الطالب البريطاني صرح أمام المحكمة أنه قام باختراق الحساب الشخصي للعامل في مؤسسة فيسبوك، ليكتشف مواقع الضعف في النظام الأمني لفيسبوك، فإن حجته هذه لم تنقذه من الحكم بالسجن لمدة ثمانية أشهر.

و هناك مدارس ومعاهد يتبعها مختبرو الاختراق منها التي تركز على تطبيقات الويب مثل OWASP ومنها الذي يركز على النظام وجمع المعلومات مثل OSSTMM وNIST ولكن في كل الأحوال تتبع خطوات ليست بالضرورة أن تكون إجبارية أثناء الاختبار ولكن هي خطوات تساعد المختبر باتباع تقنيات مجربة وأمنة في الاستخدام. يجتمع المختبر والجهة المعنية بالاختبار لتحديد خطة العمل وتحديد نوع الاختبار المطلوب وعدد الخوادم أو التطبيقات المراد اختبارها، بعد ذلك يتم توقيع اتفاقية بين كل من المختبر والجهة المعنية بالاختبار اتفاقية وتحديد موعد الاختبار و لأجهزة المستخدمة ورقم الIP للمختبر.

بعد الانتهاء من توقيع الاتفاقية يقوم المختبر بجمع أكبر عدد من المعلومات المتوفرة عبر الانترنت ويكون ذلك من خلال استخدام تقنيات في الاختراق تسمى Google Hack مع العلم ان هناك شرحا مفصلا من خلال كتيبات الكترونية لمن يريد معرفة تفاصيل أكثر.

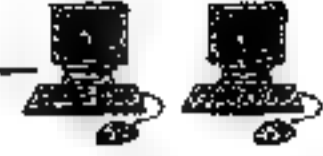


وهذه التقنية التي تستخدم محرك البحث جوجل كمساعد لها في معرفة المعلومات المتوفرة عبر الانترنت، ففي بعض الأحيان يخطئ مديرو النظام عندما يطلبوا أن ملفاتهم الموجودة على الخادم قد وضعت في مكان غير ظاهر للمستخدم هي مخفية عن متناوله، فباستخدام هذا الأسلوب وأماليب أخرى يستطيع المحترق والمختبر معرفة جميع الملفات الموجودة على الخادم الموقع، على سبيل المثال لو وصعنا التالي في محرك البحث جوجل `site:teedoz.com shehab` سوف نلاحظ أن جوجل حصر البحث في موقع كمبيوننت فقط وقام بالبحث عن كلمة `shehab` فقط. بعد مرحلة جمع المعلومات يقوم المختبر بالتعرف على الهدف المراد اختباره بشكل أكبر عن طريق مسح المنافذ الموجودة ومعرفة أنواع التطبيقات والخدمات المتوفرة في الهدف مع اتباع خطوات معينة لعرض جميع الخدمات المرتبطة بشكل مباشر وغير مباشر في الهدف.

كما يتقدم عمل المختبر ليكون أشمل وأوسع عبر تحليل التطبيقات ومعرفة عدد المتغيرات في التطبيق وقيم المتغيرات ومعرفة إصدارات التطبيقات والخدمات. في المرحلة الرابعة يقوم المختبر بتحليل النواتج من المرحلتين السابقتين ويحاول اكتشاف نقاط الضعف واستغلالها لتكوين ثغرات يطبقها فور اكتشافها لكي يثبت حقيقة وجودها في التطبيق أو النظام المختبر، في هذه المرحلة بالتحديد يقضي المختبر معظم فترة المشروع المتفق عليها باكتشاف نقاط الضعف وتحليل تلك النقاط وبرمجة برمجيات معينة إن لزم الأمر لاستثمار نقاط الضعف.

بعد الانتهاء من اكتشاف نقاط الضعف واختبارها يقوم المختبر بكتابة تقرير مفصل عن جميع المخاطر ونقاط الضعف والثغرات المكتشفة مع تقديم نصائح وإرشادات لإغلاق تلك الثغرات والنقاط بشكل مفصل وتقني وتحديد خطورة النقاط والثغرات المكتشفة عبر تصنيفها بثلاث مراتب وهي «خطورة» High متوسطة الخطورة Medium وقليلة الخطورة Low ويتم ذلك بعد الرجوع لمصادر معتمدة في تقييم المخاطر الأمنية ودراسات أمنية تتم من قبل المختبر.





اساليب القرصنة

تعدد اساليب القرصنة الالكترونية ابرزها: -

- 1 - بتقنية (SEO) وهي تقنية لوضع روابط ملوثة على رأس لائحة نتائج البحث عن الصور وتحديدًا في محرك البحث "غوغل"، فعند النقر على تلك الروابط، الملوثة في محرك البحث الذي لم يتسنى له "فلترة" النتائج، فإن المستخدم يوجه إلى موقع مضغ بما يعرف بالـ (Rogueware) أي برامج مكافحة الفيروسات المزيفة، فعند وصول المستخدم لهذا الموقع المضغ، يوهم بأن لديه فيروس أو مقطع برعجي خبيث وأن البرنامج المزيف الذي يقترحه الموقع سيخلصه من هذا التلوث، ويطلب من المستخدم تحميل برنامج اسمه «Best antivirus 2011»، ومن ثم يجبره على دفع المال لشراء هذا البرنامج الاحتيالي، وفي الواقع فإن هذا البرنامج هو برنامج خبيث يثبت نفسه في جهاز الكمبيوتر ويعمل كحاصنة طروادة.
- 2 - برنامج جاسوس إعلاني قابل للتنفيذ يعرف باسم (Hotbar) يتمثل بصور وفيديو بالإضافة إلى مقالات و معلومات عن عمليات عسكرية، وفي أسفل الصفحة رسالة مع نافذة لقارئ ملفات الفيديو من نسق فلاش يطلب من المستخدم تحميل إضافة (Plug In) لتحديث القارئ ليتمكن من مشاهدة الفيلم.
- 3 - الرسائل والروابط المتطفلة على مواقع التواصل الاجتماعي وفي لعب البريد الالكتروني، وهي روابط تنقل المستخدم عند النقر عليها إلى مواقع مضخة ببرامج خبيثة وبرامج متطفلة جاسوسة، هذا ويتوقع خبراء شركة سيمانتيك المتخصصة بمكافحة الفيروسات وأمن الشبكة موجة عارمة من البريد الالكتروني.

وعليه تنصح شركة سوفوس، المتخصصة بمكافحة الفيروسات وأمن شبكة المعلومات، المستخدمين بعدم النقر الأعمى على الروابط والوصلات في





الرسائل الالكترونية المتطفلة أو على الروابط المتطفلة المنشورة على صفحات مواقع التواصل الاجتماعي أو الروابط التي يحصل عليها المستخدم من خلال نتائج محرك البحث من دون التأكد من مصدر الرابط ومن دون قراءة وثيقة التأكد من حلو الموقع من أي تهديدات والتي تستخدمها معظم محركات البحث عند "فلتر" نتائج البحث، وبالتالي نصحت شركة سوفوس المستخدمين بعدم الموافقة على أي مسح "أمني" لجهاز الكمبيوتر، مقترح من مواقع مجهولة أو غير موثوق بها بعد وصول المستخدم إليها من دون إرادته، وبالتالي عدم تحميل الإضافات لقارئ الملفات من مواقع مشبوهة، وأخيرا التنبه إلى ضرورة التحديث الدائم لبرنامج مكافحة الفيروسات وبرنامج الجدار الناري وأيضا برامج مكافحة البرامج المتطفلة الجاسوسة في جهاز الكمبيوتر.

4 - قيام متسللين مجهولين بنسخ مشابهة لمفاتيح "سيكيوراي دي" الالكترونية من قسم "ار.اس.ايه" للسلامة في شركة "ثي.ام.سي كورب"، ويتمثل ذلك بقيامهم باختراق شبكات أمنية لشركة لوكهيد مارتن كورب وبضغ جهات أخرى متعاقدة مع الجيش الأمريكي.

ويقول خبراء تكنولوجيا انه من المستحيل عمليا على أي شركة أو هيئة حكومية بناء شبكة أمن لا يمكن للمتسللين اختراقه، وقالت وزارة الدفاع الأمريكية التي لها نحو 85 ألف عسكري ومدني يعملون على مسائل الأمن التكنولوجي حول العالم انها استخدمت أيضا عددا محدودا من مفاتيح امان ار.اس.ايه ولكنها رفضت الكشف عن المدد بالتحديد لدواع أمنية، وتمكن المتسللون من معرفة كيفية نسخ هذه المفاتيح الالكترونية ببيانات مسروقة من ار.اس.ايه خلال هجوم معقد كشفت عنه ثي.ام.سي في مارس اذار وفقا لما قاله المصدر، ورفضت ثي.ام.سي التعليق على المسألة وكذا مسؤولون تنفيذيون في جهات كبيرة متعاقدة مع الجيش الأمريكي.

5 انتحال الشخصيات والتغريب بصغار السن بل تعدت جرائمهم إلى التشهير وتشويه سمعة ضحاياهم البنين عادة ما يكونوا أفراداً أو مؤسسات تجارية





ولكن الأغرب من ذلك أنهم يحاولون تشويه سمعة مجتمعات بأكملها خاصة المجتمعات الإسلامية.

مما حدا بالعالم للتحرك حيث وقعت 30 دولة على الاتفاقية الدولية الأولى لمكافحة الإجرام عبر الإنترنت في العاصمة المجرية بودابست، وشملت المعاهدة عدة جوانب من جرائم الإنترنت، بينها الإرهاب وعمليات تزوير بطاقات لائتمان ودعارة الأطفال.

6- ولم تقتصر جرائم الانترنت على اقتحام الشبكات وتخريبها أو سرقة معلومات منها فقط بل ظهرت أيضاً الجرائم الأخلاقية مثل الاختطاف والابتزاز والقتل وغيرها.

وفي ظل التطورات الهائلة لتكنولوجيا المعلومات، ونظراً للعدد الهائل من الأفراد والمؤسسات الذين يرتادون هذه الشبكة، فقد أصبح من السهل ارتكاب أبشع الجرائم بحق مرتاديه سواء كانوا أفراداً أم مؤسسات أم مجتمعات محافظة بأكملها.

وهو مادفع العديد من المنظمات والهيئات إلى إطلاق الدعوات والتحذيرات من خطورة هذه الظاهرة التي تهدد كل مستخدمي الإنترنت حيث أصبحت أسهل الوسائل أمام مرتكبي الجريمة، فراح المجرمون ينتهكون الأعراض، ويفررون بالأطفال، إضافة إلى اقترافهم لجرائم التشهير وتشويه السمعة عبر مواقع إلكترونية مخصصة لهذا الهدف.

7- الحصول على معلومات شخصية حول مستخدمي الإنترنت.

8- والتحرش الجنسي بهم،

9- ممارسة الاحتيال عبر شبكة المعلومات الدولية.

شركة جارليك المتخصصة في مجال التأمين الإلكتروني أكدت أن عدد الحرائم الجنسية بلغ نحو 850 ألف حالة، فيما بلغت عمليات سرقة الهوية 92 ألف حالة، بينما وصل عدد جرائم الاحتيال للحصول على الأموال نحو 207 آلاف عملية.





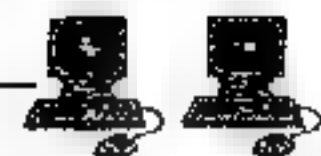
بزيادة 30 في المائة عن العام السابق، في حين تمت نحو 145 ألف عملية اختراق للحاسبات عبر الإنترنت.

أكثر أساليب القرصنة شيوعاً

من أكثر أساليب الاختراق شيوعاً في وقتنا الحالي هي الاختراقات التي تستهدف تطبيقات الويب والبرامج المساعدة في تشغيل المواقع وإدارتها كما يكون مستخدمها في موضع خطر في بعض الأحيان.

وتعود أسباب كثرة اختراقها لكثرة استخدامها من قبل مديري المواقع والصلاحيات التي توفرها بعد الاختراق. مما شجع مكتشفي الثغرات والمخترقين بالتدقيق والبحث عن نقاط الضعف في تلك التطبيقات التي فيما بعد تستثمر لتكون ثغرات جاهزة في أيدي المخترقين وأطفال السكرينات «Script Kiddies» فمن أكثر الثغرات توجد في وقتنا الحالي «Cross-site scripting XSS» و «SQL Injection» و «Cross Site Request Forgery CSRF» و «Leakage and Improper Error Handling» وهي تسرب المعلومات عن طريق الإنترنت مما يجعل مهمة المخترق سهلة بوجود ما يسمى Google Hack وهو استخدام محرك البحث جوجل في البحث عن المعلومات المتعلقة في الموقع ومحاولة كشف أي تسرب للمعلومات أو الملفات المراد إخفاؤها من قبل مدير التطبيق أو النظام، وأيضاً يمكن تسرب المعلومات عن طريق إحداث أخطاء في التطبيق مما تساعد المخترق بجمع أكبر عدد من المعلومات عن التطبيق ومعرفة طبيعة التطبيق الجدير بالذكر أن الموضوع لا يتوقف عند اختراق الموقع بل يمتد ليشمل باقي المواقع الموجودة على الخادم «server» لأن المخترقين في العادة يحاولون رفع صلاحياتهم على النظام من مستخدمين لمديري نظم Administrator في بيئة ويندوز ، و root في بيئة لينكس ويكون ذلك باستخدام ثغرات تدعى Local Root Exploit في لينكس و administrator privilege escalation في بيئة ويندوز والتي تعتمد في الغالب على أخطاء النظام نفسه أو خطأ في أحد تطبيقات المنزلة في النظام والتي تساعد





المخترقين باستغلالها ، ولو فرضنا وصادف أن يكون النظام محمياً بشكل جيد وجميع التطبيقات تخلو من الأخطاء والثغرات الأمنية يبدأ المخترقون باستخدام أساليب وطرائق أخرى مثل تحميل ما يدعى ال `phpshell` لتكون في المقام الأول أبواب خلفية لهم للعودة إلى النظام متى أرادوه وأداة للتجوال داخل الخادم واستعراض ملفات المستخدمين الآخرين ومن ثم اختراقهم.

مع الأخذ بالاعتبار أنه تم اكتشاف حل لمشكلة ال `phpshell` فيما سبق وهي عن طريق تفعيل ما يدعى `php safe mode` في أنظمة لينكس مما كان يحد من عمليات الاحترق الداخلي، غير أنه ومع مرور الوقت اكتشف المخترقون طرائق عديدة لتخطي ال `php safe mode` فكان الحل الوحيد هو تعطيل بعض الدوال الخطيرة في `php` وتغيير صلاحيات ملفات معينة مع تركيب بعض البرمجيات التي تشل حركة المخترق داخل السيرفر وتقلل الضرر على موقع واحد فقط، ولكن بقدر ما يحاول خبراء الأمن تطوير وتحسين القاعدة الأساسية للأمن يحاول المخترقون بدورهم إيجاد طرائق بديلة لتخطي الجدران المنيع، فقد كانت ال `phpshell` مثال من مئات الأمثلة لما يستخدمه المخترقون لتخطي قواعد الأمن المعدة مسبقاً من قبل مدير النظام.

صفات القراصنة

يتمتع ما يسمى بالقراصنة او المجهولون بجملة صفات منها: -

1 - أنها كيان عابر للقارات. فعلى الرغم من أنها تكونت بشكل أساسي في الولايات المتحدة وبريطانيا ، فإنها لم تحسّر بهما.

حيث إن ظروف ومكان ظهورها - الشبكة الدولية للمعلومات - جعلها فكرة قابلة للتطبيق ومنتشرة في كل الأقطار المتصلة بالشبكة العنكبوتية إذ يكفي أن يبحث الشخص عن كلمة "Anonymous" على موقع الميسبوك حتي يكتشف الكثير من الصفحات التي ترتبط فيها هذه الكلمة باسم بلد،



كأنونيموس فرنسا، وانجلترا، وهندوراس، والبرازيل، والتبت، ومصر (التي يوجد بها نحو أربع صفحات ناشطة) وغيرها.

2 - أنها لا تتكون حصرياً من مجموعة من محترفي القرصنة، أو ما يعرف بـ "الهاكرز"، ولكنها تضم في صفوفها مجموعات لديها مهارات الكتابة، وأخرى قادرة على صناعة مقاطع الفيديو، وأخرى ناشطة في الشارع، وأخرى قد لا تكون لديها أي من هذه المهارات، ولكنها تساعد في نشر المعلومات والرسائل واستساخها، خاصة على شبكات التواصل الاجتماعي.

3 - أن طبيعة "أنونيموس" غير المتجانسة معرفياً، فضلاً عن كونها ثقافية، وهو ما يجعلها غنية بالأفكار والمبادرات، ولكن كثيراً ما تكون في الوقت نفسه متناقضة المعايير والاتجاهات.

4 - رغم غياب القيادة، فإن العمليات الناجحة المؤثرة غالباً ما تسلك منهجاً معيناً يبدأ بطرح الأفكار ومناقشتها في غرفتي الدردشة الخاصتين بموقعي "Anonet" و "Anonops".

5 - قدرت هذا الكيان على الحشد، مستخدماً أساليب تعبئة شعبية كالموسيقى ومقاطع الفيديو، والرموز، والأعلام، والبيانات المطبوعة، ورسوم الجرافيتي في الشوارع، وغيرها من أدوات إعلانية يطورها المتحمسون للفكرة.

الحماية من الهاكرز

للحماية من الهاكرز لا بد من اتباع التعليمات التالية: -

1 - استخدم أحدث برامج الحماية من الهاكرز والفيروسات: وقم بعمل مسح دوري وشامل على جهازك في فترات متقاربة خصوصاً إذا كنت ممن يستخدمون الإنترنت بشكل يومي.

2 - لا تدخل إلى المواقع المشبوهة: مثل المواقع التي تعلم التجسس أو المواقع التي تحوي أفلاماً وصوراً خلية لأن الهاكرز يستخدمون أمثال هذه المواقع في إدخال





ملفات التجسس إلى الضحايا حيث يتم تنصيب ملف التجسس (الباتش) تلقائياً في الجهاز بمجرد دخول الشخص إلى الموقع))

3- عدم فتح أي رسالة إلكترونية من مصدر مجهول: لأن الهاكرز يستخدمون رسائل البريد الإلكتروني لإرسال ملفات التجسس إلى الضحايا.

4- عدم استقبال أية ملفات أثناء (الشبكات) من أشخاص غير موثوق بهم: وخاصة إذا كانت هذه الملفات تحمل امتداد (exe) مثل (love.exe) أو أن تكون ملفات من ذوي الامتدادين مثل (ahmed.pif.jpg) وتكون أمثال هذه الملفات عبارة عن برامج تزرع ملفات التجسس في جهازك فيستطيع الهاكرز بواسطتها من الدخول على جهازك وتسبب الأذى والمشاكل لك.

5- عدم الاحتفاظ بأية معلومات شخصية في داخل جهازك: كالرسائل الخاصة أو الصور الفوتوغرافية أو الملفات المهمة وغيرها من معلومات بنكية مثل أرقام الحسابات أو البطاقات الائتمانية.

6- قم بوضع أرقام سرية على ملفاتك المهمة. حيث لا يستطيع فتحها سوى من يعرف الرقم السري فقط وهو أنت.

7- حاول قدر الإمكان أن يكون لك عدد معين من الأصدقاء عبر الإنترنت وتوخي فيهم الصدق والأمانة والأخلاق.

8- حاول دائماً تغيير كلمة السر بصورة دورية فهي قابلة للاختراق.

9- تأكد من رفع سلك التوصيل بالإنترنت بعد الإنتهاء من استخدام الإنترنت.

10- لا تقم بإستلام أي ملف وتحميله على القرص الصلب في جهازك الشخصي إن لم تكن متأكداً من مصدره.

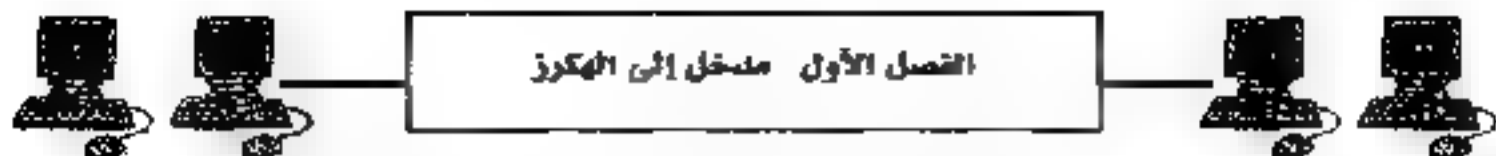
11- الحرص على جعل كلمة السر ليست كلمة شهيرة و يفضل جعلها عديمة

المعنى و اضافة بعض الارقام و لا تقل عن 8 حروف مثل s4d3lt6v او

e4gol3s6 . و وضع كلمة سر على الجهاز فهذه الكلمة حتى لو تمكن

الهكر من وضع باتش على الجهاز فإن كلمة السر تمنعه من متابعة عمله

12- ابقاف خاصية مشاركة الملفات :-



control panel / network / configuration / file and print sharring

i want to be able to give others access to my files

الفي التحديد ثم ok

هناك ثلاث طرق احترافية لحماية جهازك من الهاكرز

هناك ثغرات في أجهزة الاكس بي دائما تكون مدخل للهاكرز ومعظمها

لايعرفها

1- الثغرة الأولى :

تعتبر إحدى البوابات الخطرة للفايروسات وملفات التجسس :

1- لوحة التحكم control panel

2- خيارات المجلد folder options

3- أنواع الملفات file types

وهناك أبحثو من:

'Windows script host setting file'

واحذفوه على الفور

2- الثغرة الثانية:

اسمها (مشاركة ملفات بسيطة) simple file sharing

لكن تفعيلها مش بسيط بل هو خطير جدا.

1- خيارات المجلد folder options

2- عرض view

3- يجب إزالة علامة الصح من داخل المربع أمام: مشاركة ملفات بسيطة

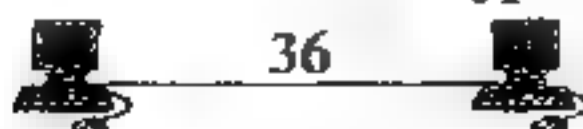
(مستحسن).

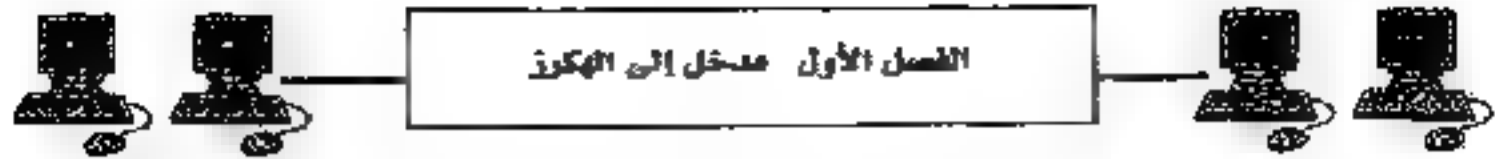
(use simple file sharing) (recommended)

3- الثغرة الثالثة :

اسمها: ((عدم حفظ الصفحات المشفرة إلى القرص)).

save encrypted page to disk





والطريقة كالتالي:

1- لوحة التحكم control panel

ثم Network and Internet Connections

2- خيارات انترنت ineternet options

3- خيارات متقدمة advanced

4- وضع علامة صح داخل المربع:

((عدم حفظ الصفحات المشفرة إلى القرص))

don't save encrypted page to disk

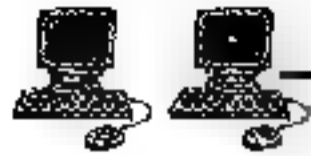
ثم موافق.

كيف تقع ضحية الهكرز (القرصنة)

أولاً: التنصت بلوحة المفاتيح اللاسلكية: قامت شركة Remote-exploit.org المتخصصة في تصميم منتجات الحماية الأمنية بإصدار تصميم أجهزة مفتوحة المصدر وبرامج مصاحبة لجهاز يقتنص ثم يفك شفرة إشارات تصدر من لوحات المفاتيح اللاسلكية.

ويستخدم الجهاز قطعة استقبال لاسلكية يمكن إخفاؤها في الملابس أو يتم تغيير هيئتها، ومن ثم يمكن تركها فوق مكتب قريب من جهاز الكمبيوتر لالتقاط الإشارات. وتستهدف تلك التكنولوجيا التي يطلق عليها Keykeriki لوحات المفاتيح اللاسلكية التي تعمل بـ 27 ميغاهيرتز لاستغلال انعدام الأمان الذي اكتشفته شركة Remote-exploit.org في وقت مبكر.

ثانياً: التنصت بلوحة المفاتيح السلكية: تمر النبضات الكهربائية عبر النظام التي تولدها لوحات المفاتيح للإشارة إلى المفتاح الذي يتم الضغط عليه عبر النظام الأساسي للوحة المفاتيح والحاسوب نفسه وكذلك قاعدة شبكة الأسلاك الكهربائية في المنى الذي يوصل به الحاسوب. كما يمكن للتحقيقات التي تُجرى



على أرض الواقع للأسلاك الكهربائية أن تلتقط تلك التقلبات الكهرومغناطيسية، ويمكن الحصول عليها وترجمتها إلى حروف.

و تُعرف القدرة الخاصة بتلك النوعية من التقنيات منذ عشرات السنين، ويعتقد كثير من الخبراء أن وكالات التجسس قامت بتحسين التقنيات التي جعلت هذه النوعية فاعلة من الناحية العملية. هذا وقد قام كل من أندريا باريساني ودانييلي بيانكو، الباحثان بمؤسسة Inverse Path المتخصصة في أمن الشبكات، بتقديم بحثهم السريع والقدر في الوقت نفسه حول الموضوع في مؤتمر القبة السوداء هذا العام بالولايات المتحدة، أملاً في إثارة المزيد من الأبحاث حول تلك التقنيات

ثالثاً: التقصت بأجهزة اللابتوب بوساطة الليزر. صدور أشعة الليزر "الانقضاخية" عن أجهزة اللابتوب، والاستيلاء على الاهتزازات التي تحدث في الوقت الذي يتم لضبط فيه على المفاتيح، كل هذا يمنع المهاجمين قدرًا كافيًا من بيانات للاستدلال على ما تتم كتابته.

مع ملاحظة أن كل مفتاح يصدر عنه مجموعة فريدة من الاهتزازات تختلف عن تلك التي تصدر عن أي مفاتيح أخرى.

أما مفتاح المسافة فتصدر عنه مجموعة أخرى إضافية فريدة، حسبما قال باريساني وبيانكو، ويمكن أن تساعد برمجيات تحليل اللفة في تحديد نوعية مجموعة الاهتزازات التي تقابل ما يناظرها من مفاتيح، وإذا ما عرف المهاجم اللفة التي يتم استخدامها، فيمكن الكشف عن الرسالة.

رابعاً: برامج الـ **keyloggers** التجارية: النماذج الأولية منها عبارة عن أجهزة يتم توصيلها في لوحات المفاتيح، لكنها تطورت حتى أصبحت أدوات برمجية يمكنها أن تلتقط ما يتم كتابته على لوحة المفاتيح ونحريه أو إرساله لأحد السيرفرات لهجومية. وتمتلك النسخ التجارية البرمجيات المحملة على ذاكرة (فلاش) التي يمكنها التخلص من البرامج على الكمبيوتر ثم يُعاد إدخالها بعد ذلك لتحميل البيانات التي تم تحميتها.





خامساً: الهواتف المحمولة: بإمكان البرمجيات التي يتم تحميلها على موديلات معينة من الهواتف المحمولة أن تسكت قارعي الأجراس وتقطع العروض الصوتية التي عادةً ما تحفز عند استقبالهم للمكالمات. ويمكن للمتصل أن يستمع آنذاك للمحادثات بداخل الغرفة التي يوجد بها الهاتف. ووفقاً لتقارير صحفية، فقد حصل مكتب التحقيقات الفيدرالي FBI على إذن قضائي لاستخدام تلك التقنية في التجسس على أعضاء المافيا المشتبه فيهم بنيويورك.

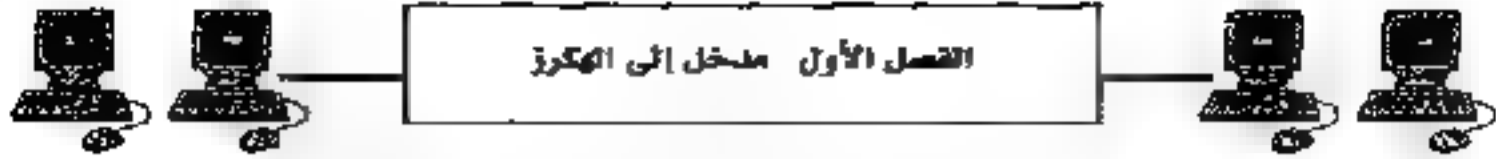
سادساً: شريحة الهاتف المحمول: إذا تمكن المهاجمون من الحصول على أحد الهواتف المحمولة لفترة قصيرة، فسيكون بإمكانهم استخدام برمجيات متاحة من الناحية التجارية لتحميل وقراءة الشرائح ومخزونهم من أرقام الهواتف، وشعارات الاتصالات، والرسائل القصيرة، والصور، وغيرها من الأشياء.

سابعاً: التنصت بإنقاذ القانون المبني على نسخ الصوت: تشتمل مفاتيح صوت شركة الهواتف المحمولة على برمجيات يمكنها البحث في جميع المحادثات التي تتم من خلالها عن الأصوات التي توافق مجموعات الطباعة الصوتية.

وقال جيمس أتكينسون، الخبير في إجراءات المراقبة التقنية المضادة، أنه وفي كل مرة يحدث فيها توافق، فإن ذلك من الممكن أن يؤدي إلى تسجيل المحادثة وتبنيه مسؤولي إنقاذ القانون.

ثامناً: الاستيلاء عن بعد على بيانات الكمبيوتر: بموجب التقنية الواضحة التي يطلق عليها عنوان بروتوكول الإنترنت للمحقق (CIPAV)، قام مكتب التحقيقات الفيدرالي FBI بتعقب بيانات الحواسيب الشخصية عن بُعد. هذا ولم يتم الكشف من قبل عن تفاصيل تلك التكنولوجيا على الإطلاق، لكن تم استخدامها لتعقب طلاب المرحلة الثانوية الذين قاموا بإرسال تهديدات بوجود قنابل عبر البريد الإلكتروني. كما تقوم تقنية (CIPAV) بالاستيلاء على عناوين الـ IP وأجهزة الماك، وإدارة العمليات، والمواقع الإلكترونية التي تمت زيارتها، وإصدارات أنظمة التشغيل، والمالك المسجل، وتدوين تفاصيل الكمبيوترات التي تُوصَل بها الكمبيوترات المستهدفة.





تاسعاً: التلفزيون الكيبل كشبكة يمكن استغلالها والاستفادة منها: يقول جيمس أتكينسون أنه ونظراً لإمكانية تمحور معظم شبكات التلفزيون الكيبل، فإن أي إيماءة يمكنها مراقبة حركة أي إيماءة أخرى وعلى العموم، يعتبر الأمن أمراً بدائياً، كما أن التشفير المستخدم يمكن أن يتعرض للقرصنة على يد أحد الأشخاص من خلال مهارات تقنية أساسية وأدوات متاحة ومتوافرة لك لشفرة، على حد قول أتكينسون.

عاشراً: مراقبة الهاتف المحمول: تزعم البرمجيات المتاحة من الناحية التجارية أنها تستولي على المحادثات والرسائل الخاصة بالهاتف المحمول، ويحتاج المهاجمون إلى الوصول بشكل مادي إلى الهاتف بغرض تحميل البرمجيات التي تمكنهم من ذلك، وهناك العديد من الممارسات التجارية الخاصة بتلك البرمجيات في السوق، لكن تنتشر شكاوى على الإنترنت من أن البرمجيات لا تعمل بنفس الشكل الذي يروج به في الإعلانات، أو أن يكون استخدامها أكثر تعقيداً إذا ما تجاوز المدى الذي يسمح به الباعة.

أشكال القرصنة

تعدد أشكال القرصنة الالكترونية وتوسع مدياتها إلا أننا سنحاول ان نتحدث عن بعض هذه الاشكال ومنها :-

1 - القرصنة الهاتفية

المقصود بالقرصنة الهاتفية هنا هو إجراء مكالمات هاتفية دون تسديد أجرة المكالمات، ويتم ذلك باستعمال "علب الكترونية" تحول دون عمل معدات احتساب المكالمات. وهذه العلبة هي:

"علبة سوداء" (Black Box) وهي تقلد إشارات الموجات المتعددة المستعملة في الاتصالات الهاتفية على المدى البعيد، وهو ما يجعل إشارة القرصنة تبدو وكأنها إشارة لبدالة تحويل الاتصالات.



وتوضح الدراسات الحديثة الدور الذي لا غنى عنه للهواتف المحمولة عموماً، والرسائل النصية، على وجه التحديد، في حياة المراهق الأمريكي، وحد أن واحداً من ثلاثة مراهقين، يرسل أكثر من 100 رسالة نصية في اليوم وخلص الاستطلاع الذي أجراه مركز بيو للأبحاث، إلى أن ثلاثة أرباع المراهقين الأمريكيين، ممن تتراوح أعمارهم ما بين 12 إلى 17 عاماً، يفتنون هواتف محمولة، بارتفاع بلغت نسبته 45 في المائة عن معدل عام 2004 ولفت الاستبيان، إلى تزايد سريع ومطرد في معدل تبادل الرسائل النصية خلال الآونة الأخيرة.

ويبدو واضحاً للعيان، تهقر معدل المكالمات الهاتفية لصالح الرسائل النصية، ولجأ الشباب للمكالمات الهاتفية للتواصل مع الآباء غير أنهم يفضلون التغاطب عبر الرسائل النصية مع الأصدقاء.

ورغم تلقيهم أو إجرائهم لما بين خمسة مكالمات يومياً، وجد البحث أن نصف المراهقين يرسلون نحو 50 رسالة نصية في اليوم. بحسب سي أن ان.

أماندا لينهارت، كبير الباحثين فسرت هذه النتائج بالقول: "الرسائل النصية فعالة ومريحة وتتسجم مع هذه المساحات الصغيرة في الحياة اليومية.

لا تتحدث فيها كثيراً، وتدلل بها للناس أنك مازالت متواصلاً ومرتبطة بهم." وحول كيفية تمكن المراهقين من تبادل هذا الكم من الرسائل النصية

وهم يقضون معظم يومهم داخل الفصول الدراسية، وجد المسح أن 43 في المائة من الشباب يأخذون هواتفهم المحمولة إلى المدرسة، وأن رسالة نصية واحدة على الأقل،

ترسل من داخل الفصل، رغم حظر معظم المدارس على التلاميذ حمل الهواتف. ربما تكون التقنية الحديثة قد وفرت لنا الهواتف المحمولة وطرق الاتصال

الحديثة لكنها تسببت أيضاً في الكثير مما يثير الغضب ويسبب للآخرين. و صبحت الهواتف المحمولة عنصراً ضرورياً في حياتنا المهنية والشخصية على

السواء لكن هناك أيضاً قواعد سلوكية يجب اتباعها عند استخدامها.



وتتطلب اللياقة الجيدة في استخدام الهاتف المحمول القليل من الجهد او التفكير فهي ببساطة تدرك ما يحيط بك وأن تحترم الآخرين. فإذا كنت تشعر بالحرج من نغمة رنين هاتفك في مواقف معينة مثل أثناء وجودك في القطار او العمل فهي بالتأكيد خيار خاطيء.

ودرجة رنين النغمات يجب الا تكون مزعجة. اغلق هاتفك المحمول او اضبطه على خاصية الاهتزاز عندما تحضر اجتماعات او تكون في المسرح او دور السينما وما شابه ذلك.

أيضاً الهاتف المحمول ليس مكبر صوت لذا لا تصيح وانت تستخدمه وكن على دراية بما حولك ولا تحاول استخدام هاتفك في مواقف يمكن ان تزعج فيها آخرين فالصوت المرتفع يمكن أن يصرف انتباه ركاب يقرأون الصحف في عربة قطار هادئة او يبدو تطفلاً على حافلة مكتظة بالركاب.

ومن غير اللائق اجراء معادئات حميمة امام الآخرين. وبالمثل لا تستخدم لغة فظة كما يجب تجنب الحديث عن المال او الجنس في حضور آخرين. ويتحتم احترام خصوصيتك وخصوصية الآخرين.

وهناك اماكن محددة من غير المقبول فيها استخدام الهاتف المحمول مثل المعارض الفنية وأماكن العبادة والمكتبات والمستشفيات.

وبما أن الانسان يستحق المزيد من الاهتمام أكثر من الآلة يجب اغلاق هاتفك قدر الامكان في المناسبات الاجتماعية. ولا تضع هاتفك على طاولة الطعام ولا تنظر اليه في منتصف حديثك مع الآخرين.

هإذا ما كنت تنتظر اتصالاً مهماً عندما تقابل شخصاً ما في مناسبة اجتماعية فاشرح له في البداية أنك سترد على اتصال واعتذر سلفاً.

كما وانتشرت مؤخراً استقبال الاجهزة الخلوية الخاصة بالعديد من المواطنين رسائل قصيره (SMS) محتواها ان صاحب الرقم قد فاز بمبلغ خيالي من خلال عماره تاتي بالصيغة التالية (congratulations your mobile number has won 170.000.00 bounds in the on going nokia mobile





promo for claim call 0034-693-361-112 or e-mail: nokia 1798
@yahoo.com) او بعبارة مشابهة وعناوين مختلفة.

وحيث أن الشركات الخلوية المختلفة لم تقم بإجراء مثل هذه المسابقات وأن مصدرها من إحدى الدول الإفريقية وتعتبر أسلوب احتيالي جديد من خلال سرقة معلومات الأشخاص الذين يقومون بالاتصال بالأرقام والعناوين الميينة في الرسائل القصيرة لغايات استخدامها في عمليات احتيالية إلكترونية، كما هو الحال بمرور مكالمات من أرقام دولية يعتمد المتصل منها إلى تكرار الاتصال دون ترك مجال للمستقبل لكي يجيب لتثير حب الفضول لديه و يقوم بإعادة الاتصال بهذه الجهة والتي في الأغلب يقدم نفسه على أنه يقطن في بلد إفريقي واقع تحت ويلات الحروب والمجاعات ويحاول البحث عن من يساعده في تصريف أموال قد ورثها عن والديه أو اختلاق قصص من هذا القبيل لغايات تأمين أمواله مقابل تحويل العملة من بلده بمبالغ أقل من سعرها الحقيقي بكثير.

ويرى تقرير صادر عن مؤسسة "جورجيا تيك" الأميركية بأن أجهزة الهاتف المحمول تشكل فرصة للقراصنة أفضل من الحواسيب لتسهيل عمليات القرصنة، وذلك لارتباطها بشبكة الاتصالات طوال الوقت من جهة، ولصعوبة تحميل برامج واهية من الفيروسات لاستهلاكها المفرط للكهرباء من جهة أخرى، وهو عامل مهم في الهواتف المحمولة.

وسيشكل النظام الأمني ومعرفة كيفية عمل شبكات الهاتف المحمول، وتكثيف الهجمات الفيروسية مع طريقة عملها تحد واضح أمام قراصنة الهاتف، وذلك لقوة النظام مقارنة بما تتبعه شركات الانترنت، مما يجعل اختراقه أصعب، كون شبكات الهاتف المحمول تستطيع إغلاق الخطوط الموبوءة بشكل أسهل.

وبحسب التقرير فإن نجاح القراصنة في غزو الهواتف المحمولة سيمنح أمامهم دماً واسعاً للربح المادي، من خلال دفع الهواتف للاتصال بأرقام معينة مرتفعة البعرة أو إجبارها على شراء رنات خاصة بأثمان مرتفعة، مما يعود على شركات يقوم القراصنة بتأسيسها بإيرادات مالية مرتفعة.



2 - قرصنة البرامج المحلية

هذه القرصنة هي كناية عن تجاوز البرمجيات التي توصل للحيلولة دون اختلاس نسخ البرامج الكمبيوترية التطبيقية (أي بصورة غير مأذونة).

ولقد بدأ ازدهار هذا النوع من القرصنة في الثمانينات في بلغارب، حيث كان القراصنة يقومون بنسخ البرامج الكمبيوترية الغريبة لإعادة تصديرها إلى سائر بلدان أوروبا الشرقية. وكثيراً ما يقوم هؤلاء القراصنة أنفسهم بتطوير فيروسات كمبيوترية جديدة أيضاً.

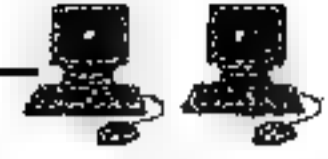
ومعظم القراصنة من هذه الفئة في البلدان الغربية هم إما تلاميذ ثانوية مولعون بألعاب الفيديو، أو طلاب جامعيون، والصفة الغالبة أنهم من المولعين بالكمبيوتر والتكنولوجيا الالكترونية ويؤمنون بوجود مجانية استعمال الشبكات الكمبيوترية على أساس أن ذلك يسهل عملية اتصال الناس ويوثق العلاقات الاجتماعية والصداقة بين الأمم والشعوب.

وفقاً لشركة بت ديفندر فإن البرمجيات الخبيثة ستزيد بنسبة 23% في عام 2012 إلى 90 مليون عينة، أي أكثر بحوالي 17 مليون مقارنة بنهاية عام 2011.

هذه البيانات تشكل جزءاً من تقرير بتديفندر حول التهديدات الالكترونية، والذي يتطلع إلى المستقبل ويتوقع تطور البرمجيات الخبيثة على الشبكات الاجتماعية مثل الفيسبوك وتويتر وحتى على أجهزة الهواتف المحمولة بالإضافة إلى نمو الجريمة الالكترونية.

يتوقع التقرير أيضاً أنواعاً جديدة من البرمجيات الخبيثة والاحتيال الالكتروني التي تركز على الشبكات الاجتماعية في 2012، بينما ستزيد البرمجيات الخبيثة المصممة خصيصاً لأنظمة أندرويد عدد التهديدات ضد الهواتف الذكية والأجهزة اللوحية.

ومع بداية عام 2012 شهدت البرمجيات الخبيثة نمواً هائلاً، و يعود ذلك إلى انتشار الشبكات الاجتماعية و اغراءاتها، "يقول محلل التهديدات الالكترونية في بتديفندر Bogdan Botezatu، والذي قام بتحرير هذا التقرير. "سيزداد عدد



البرمجيات الخبيثة المخصصة لنظام أندرويد يشكل ملحوظ لكن بدءاً من قاعدة أقل بكثير من البرمجيات الخبيثة.

هذا التقرير هو حصيلة عام كامل من الكشف و الحماية و الازالة للبرمجيات الخبيثة حول العالم، كما انه يتضمن مراجعة لأكثر 10 برمجيات خبيثة خطورة في عام 2011، بالإضافة الى تغطية عن حركات الاختراق و سوء استغلال الشهادات الرقمية. و يشمل التقرير ايضاً تحليلاً للرسائل الالكترونية المزعجة و التي شكلت 75.1٪ من عدد الرسائل الالكترونية المرسلة حول العالم العام الماضي.

وكشفت دراسة أجراها «اتحاد منتجي برامج الكمبيوتر التجارية» بمصر، عن أن سوق البرمجيات بالبلاد تخسر نحو 1.900 مليار جنيه مصري (حوال 400 مليون دولار أميركي) كل عام بسبب عمليات «القرصنة»، مشيرة إلى أن مستوى قرصنة البرمجيات فيها يصل الى 67٪، وأن نسبة البرامج المرخصة لا تتعدى 33٪ من إجمالي البرامج المستخدمة، مؤكدة أن الفاقد في عائدات الضرائب بلغ قرابة 415 مليون جنيه (83 مليون دولار)، والفاقد في فرص العمل 2.5 مرة مقارنة بالحدالي ونهت الدراسة التي أجرتها شركة «ايبه نيلسون عامر» لصالح الاتحاد مؤخراً لمدة شهر كامل، متخذي القرار في 461 شركة صغيرة ومتوسطة الحجم في القطاع الخاص، أن هناك حوالي 50.000 شركة تملك على الأقل جهاز كمبيوتر واحد، وقدرت معدلات اختراق الكمبيوتر بنحو 38٪، موضحة أن الشركات المتوسطة (4.25 ألف شركة) تملك كل شركة منها في المتوسط نحو 52 جهازاً، أما الشركات الصغيرة 10.800 ألف شركة) فمتوسط أجهزة الكمبيوتر لديها يصل إلى 9 أجهزة، والشركات الصغيرة جداً (34.200 ألف) يصل المتوسط بها إلى 4 أجهزة لكل شركة.

وحذرت الدراسة من أن سوق البرمجيات المصري يتكبد خسائر ضخمة، بسبب انتشار النسخ غير القانونية من البرامج، وأن الخسائر لا تقتصر على الشركات المنتجة للبرمجيات، وإنما تمتد إلى الاقتصاد وسوق العمل، لافتة إلى أنه



على الرغم من أن مصر تأتي في الوسط بين دول تتخفّض فيها معدلات القرصنة مثل الولايات المتحدة (20%) ودول ترتفع بها تلك المعدلات مثل فيتنام (90%)، إلا أنه من الممكن أن تتخفّض تلك المعدلات إذا ما باشرت الأجهزة الرقابية دورها.

3 - الارهاب الإلكتروني

يعد الارهاب الإلكتروني شكلا من اشكال القرصنة وقد يعرف بأنه استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين. أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية.

ويعرفه الباحثون بأنه: - "نشاط هجومي متعمد ذو دوافع سياسية بغرض التأثير على القرارات الحكومية أو الرأي العام باستخدام الحاسبات ووسائل الاتصال للتأثير على إنتاج ومعالجة وتخزين المعلومات أو تعطيل خدمات. وينتج عنه ترويع وتخويف وتدمير للبنية التحتية الحيوية ومن خلال ثلاثة أبعاد هامة

- يتمثل أولها في أن يصبح الانترنت عاملا مساعدا للعمل الإرهابي التقليدي المادي بتوفير المعلومات عن الأماكن المستهدفة أو كوسيط في عملية التنفيذ.

- أما البعد الثاني فهو ما يعد تأثيرا معنويا ونفسيا من خلال التحريض على بث الكراهية الدينية وحرب الأفكار.

- أما البعد الثالث فيتم في صورة رقمية من خلال استخدام آلياته الجديدة - الفيروسات - في معارك تدور رحاها في الفضاء الإلكتروني والتي قد يقتصر تأثيرها على بعدها الرقمي أو قد تتعدى لإصابة أهداف مادية".

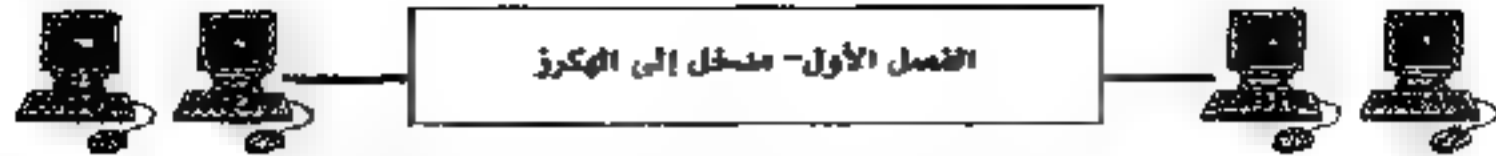
هذا وقد سهلت التكنولوجيا الحديثة عمل الارهاب الإلكتروني من

خلال:-

1 - أصبح الإرهاب الإلكتروني مادة يومية لتناول الصحف وغيرها من وسائل

الإعلام وذلك إما بهدف الإثارة وجذب الجمهور أو بهدف البحث عن المعرفة الحقيقية حول ذلك الخطر، وخاصة مع فشل وسائل الإعلام في التفريق بينه وبين غيره من المفاهيم والتي تصلح جميعا للتعبير عن الإرهاب الإلكتروني طالما يتوقف ذلك على طبيعة الدافع "السياسي" من وراء حدوثها.





2 - اثر الجمع بين الإرهاب والتكنولوجيا على الشركات العاملة في مجال تكنولوجيا المعلومات، والذي يدفعها الخوف من التأثير على درجة توسع أسواقها إلى الاستثمار في الخدمات الأمنية التكنولوجية من جانب وإلى المنافسة الشديدة من جانب آخر بين الشركات العالمية، وضغطا على نفقاتها في البحث والتطوير.

3 - استغل بعض السياسيين الخوف من الإرهاب الإلكتروني في ممارسة مزيد من إرهاب مواطنيهم بهدف تمرير قوانين معادية للحريات المدنية وتشكيل انتهاكا للخصوصية، وخاصة بعد أحداث 11 سبتمبر كالإجراءات التي اتخذتها الإدارة الأمريكية في مراقبة البريد الإلكتروني وحجب مواقع الانترنت.

4 - لم تبق قضية الإرهاب الإلكتروني فقط سياسية بل أصبحت ذات أبعاد اقتصادية هامة، سواء من خلال الخسائر المالية الضخمة التي قد تطول البنوك والصفقات المالية الدولية وأسواق المال ومحطات الطاقة والحكومات الإلكترونية، أو تأثير ذلك على الاقتصاد الرقمي الجديد الذي أصبح يشكل جزءا كبيرا من الناتج القومي الإجمالي للدول المتقدمة.

وفي الولايات المتحدة الأمريكية بدأ مكتب التحقيقات الأمريكي الـ إف بي أي "الاستعانة بقراصنة الكمبيوتر لمساعدتهم في مكافحة الجريمة والإرهاب من خلال الدخول على أجهزة المستخدمين ومراقبتهم على الشبكة الدولية وهو ما يعتبره بعض الخبراء نوعاً من أنواع قمع الحريات.

ويؤكد عملاء فيدراليون أن المرحلة المقبلة من مكافحة الإرهاب والجريمة ستتطلب الاستعانة بأذكي العقول التقنية لخوضها، وأن هذه العقول ستوفر مبالغ ضخمة تضطر الحكومة لدفعها إلى القطاع الخاص.

ويسعى العملاء الفيدراليون بالوصول إلى تكنولوجيا تتيح لهم أن يتعرفوا على هويات مستخدمي الانترنت ومعرفة ما يفعلونه.



وهو ما دفع مكتب التحقيقات الامريكى استغلال المؤتمر الدولى "ديفكون" للقراصنة المتعقد في لاس فيجاس للبحث عن كوادز من القرصنة تساعد على اختراق أجهزة الكمبيوتر والدخول على المواقع وغيرها من عمليات القرصنة التى قد تفيدهم فى الحد من عمليات الإرهاب.

وشارك 6 آلاف من القرصنة ومخترقي الكمبيوتر في هذا المؤتمر، الذى ضم ألعاباً ومسابقات وبحوث لاختراق أجهزة كمبيوتر ومواقع انترنت وقرصنة برامج وأفضال حقيقية وصرح كبير محطلي الاختراق في وكالة الأمن القومي الأمريكية توني سيجر أن الوكالة تعرض مشاركة المعلومات للعامة على أمل أن تكسب مخترقي الكمبيوتر كعفاء في مجال الأمن الرقمي.

وأضاف "أعتقد بأننا جزء من مجتمع أكبر، وفي الأيام الخوالي كنا الوحيدين الذين نبحث في هذا المجال، وكانت أهمية اكتشافاتنا تتبع من أنها الوحيدة، أما الآن، فقلت أهمية اكتشافاتنا وزادت أهمية اكتشافات الآخرين.

فان هناك عدد من الناشطين عبر المواقع الاجتماعية كالفيسبوك والتويتر وتيفت وغيرها ينادون لانشاء صفحات لتوعية روادها بخطر القرصنة ونشر ثقافة حقوق التأليف، وهي فكرة رائعة ورائدة وبامكانها نقل الفكرة وايصال الرسائل لعشرات الآلاف من مرتادي هذه المواقع والى مختلف انحاء العالم، وبالتالي نكون قد حاربنا هذه الجريمة الالكترونية بطريقة الكترونية زيادة الى ضرورة الابلاغ على أي موقع ينشر مثل هذه الأفكار والنصح والارشاد لعدم استعمال المعلومات الواردة اليها منه، مع محاولة التبليغ عن الصفحة في الموقع لأكبر قدر ممكن من الشباب باعتبارها، لفئة الأكبر استعمالاً للأنترنت، وهذا لا يعني بأننا نستطيع التخلي عن الطرق التقليدية في دحر ظاهرة القرصنة وحماية حقوق المؤلف بل يبقى للمدرسة والجامعة والمسجد والاعلام التقليدي دوره كذلك، في ترسيخ الفكرة لان المشكل في لعالم وسيماء الدول العربية في الذهنيات ولا بد من التركيز عليها جيداً.





وسائل الارهاب الالكتروني :-

البريد الالكتروني :

إن المجرمين استخدموا البريد الالكتروني كوسيلة للتواصل فيما بينهم وتبادل المعرفة والخطط وخاصة في الآونة الأخيرة كما تم استخدامه في عمليات السرقة والتجسس على الآخرين للوصول إلى معلومات تفيدهم في عملياتهم الإرهابية،
المواقع الالكترونية :

يقوم الإرهابيون بنشر أفكارهم المضللة وخططهم والدعوة إلى الإرهاب عن طريق هذه المواقع . وقد انتشر العديد من المواقع التي تقوم بتعليم كيفية الاختراقات بمختلف أنواعها وكيفية القيام بالعمليات الإرهابية وطرق صناعة المتفجرات ونشر الفيروسات وغيرها

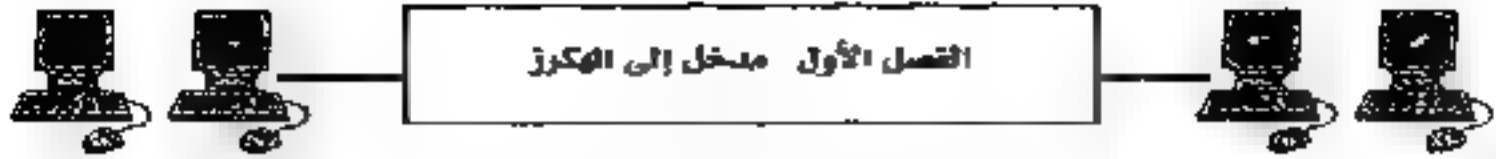
فقد وصل عدد المواقع التي تنشر الإرهاب بمختلف أنواعه إلى أكثر من 22 مليون موقع. وقد سهلت طرق الالتقاء بين الإرهابيين وأصبح العديد يطلعون على مثل هذه المواقع في نفس الوقت مما أدى إلى انتشار هذه الجرائم بكثرة.
تدمير المواقع :

ويتم تدميرها بإرسال العديد من الرسائل الالكترونية من أجهزة مختلفة إلى الموقع المستهدف للتأثير على السعة التخزينية للموقع، فتشكل هذه الكميات الهائلة من الرسائل الإلكترونية ضغطاً يؤدي في النهاية إلى تصحير الموقع العامل على الشبكة وتشتت البيانات والمعلومات المخزنة في الموقع فتنتقل إلى جهاز السارق، أو تمكنه من حرية التحول في الموقع المستهدف بسهولة ويسر، والحصول على كل ما يحتاجه من أرقام ومعلومات وبيانات خاصة بالموقع المعتدى عليه وهذه الطريقة تسمى (DDOS).

المجرمون يفضلون استخدام أساليب الإرهاب الالكتروني بدلا من الإرهاب التقليدي بسبب العديد من المزايا ومنها :

- أرخص وأدق من الطرق التقليدية.





- عدم معرفة شخصيات المجرمين ومواقعهم.
 - لا توجد حواجز مادية.
- يستطيعون عمل هذا الإرهاب عن بعد ومن أي مكان في العالم.
- تؤثر على عدد كبير من الناس وتستهدف العديد من المواقع

آثار الإرهاب الإلكتروني

وتشمل:-

1 - آثار مباشرة ومنها:-

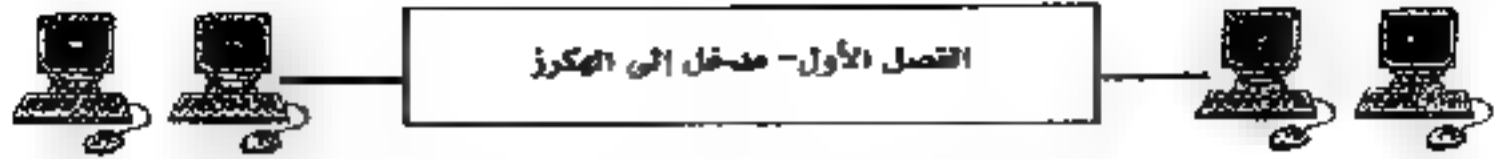
- فقدان المبيعات.
- فقدان الملكية الفكرية.
- زيادة تكاليف التأمين.

2 - آثار غير مباشرة ومنها:

- فقدان الثقة والمصداقية في أنظمتنا المالية.
- العلاقات المتوترة بين الشركاء في الأعمال.
- فقدان الثقة في الحكومة وصناعة الكمبيوتر.

الحماية من الإرهاب الإلكتروني :

- إصدار أنظمة تحد من نشوء جرائم الإرهاب الإلكتروني، وذلك بتحديد تلك الجرائم والعقوبات المقررة لها.
- تطوير البرمجيات المستخدمة في الشبكة، سواء المخصصة لأجهزة الأفراد أو الأجهزة المغذية لشبكة الانترنت وهو ما يطلق عليها بالخادم (Servers)..
- تطوير طرق تشفير المعلومات وحفظها من قبل المتخصصين وشركات إنتاج برامج الحماية.
- تنظيم الندوات والمحاضرات التي تهدف إلى توعية مستخدمي التقنية بالمخاطر المحدقة بهم.



وجود رقيب صارم يقيم مواقع الانترنت بحسب محتواها، وبناءً على ذلك يحدد إذا ما كانت قابلة للعرض أو لا.

- إثراء محتوى الشبكة العنكبوتية بالأفكار السامية والمنحصرة التي تدعو إلى السلام والمحبة والتعايش السلمي بين الحضارات المختلفة.

الارهاب الالكتروني والقرصنة الالكترونية

التشابه والاختلاف

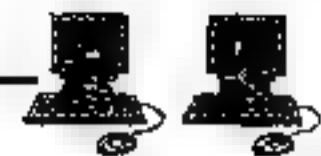
يشارك الارهاب الالكتروني مع جرائم الحاسب كالقرصنة والجريمة الالكترونية في:-

- 1 - استخدام أجهزة الحاسب.
- 2 - وتنوع الأهداف والوسائل والأشخاص والفاعلين.
- 3 - صعوبة التمييز بين استخدام تكنولوجيا المعلومات كسلاح أو هدف للهجوم.

وتتمثل عناصر الارهاب الالكتروني ب:-

أولاً: الإرهابيون الذين يستخدمون الانترنت في التجنيد والتعبئة والتخطيط والتنسيق والتمويل وجمع المعلومات حول تنفيذ العمل الإرهابي كسلاح وهدف أعدائها، وتمثل حالة تنظيم القاعدة نموذجاً لاستخدام الجماعات "الإرهابية" للمضاء الالكتروني.

ثانياً: الدول القومية، قد تستخدمه الدولة ككأداة للحرب ضد دول أخرى معادية أو في مجال الاستخبارات المعادية ضد الدول الأخرى أو قد تقوم الدول بالتعاون مع جماعات إرهابية أو أفراد للإضرار بدولة أخرى، وقد حدث هجوم الكتروني روسي على استونيا تسبب في شل حركة البنية التحتية جراء خلاف حول نقل تمثال من العهد السوفييتي، ووجهت أصابع الاتهام للصين في حدوث اختراق للبنتاغون ولأربع وزارات ألمانية ووزارة الدفاع الفرنسية.



ثالثا: المتعاطفون مع الإرهابيين أو مواقف الدول، فإتاحة شبكة المعلومات الدولية للعديد من الأفراد والدول والجماعات على الاتصال والتواصل والتأثر يدفع الى إمكانية مساهمة أي منها لمساندة دولة أو جماعة اوحتى احتجاج على قضية ما، مع تو فر درجة التشابك العالية والاعتماد المتبادل بين دول العالم بالإضافة إلى انه لا تخلو دولة من وجود مهاجرين ينتمون إلى دول أخرى أوبناء شبكة موالين ومتعاطفين مع قضية ما مع بروز قضايا يتفاعل معها الأفراد عالميا ويعيدا عن وجهات النظر الرسمية

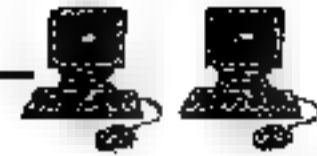
رابعا: الجريمة المنظمة، حيث قد تستغل آليات الإرهاب الالكتروني في تحقيق أهداف مادية أو مالية أو بالتعاون مع المنظمات الإرهابية في تحقيق أهدافها مقابل حصولها على المال ككالمنظمات العاملة في غسيل الأموال أو تجارة المخدرات أو السلاح.

خامسا: الباحثون عن الشهرة، فقد يقوم احد الأشخاص أوالمجموعات باستخدام آليات الإرهاب الالكتروني بهدف الشهرة من قبل أشخاص ذوي درجة عالية من الذكاء، وعلى الرغم من إن الأنواع الأربعة السابقة قد ترتبط بالإرهاب بشكل مباشر وغير مباشر إلا أن هذا النوع الأخير قد لا يمكن ادخاله في العمل الإرهابي.

سمات الإرهاب الالكتروني

يعد الحاسب الآلي هو الفاعل الوحيد الذي يبقى في منأى عن التمرض للخطر، كما ان العمليات تتم عبر شبكة الانترنت لما تتميز به:

- 1 - رخص تكلفة الدخول.
- 2 - كما يتميز من يقوم بمثل هذه الهجمات بأنه شخص ذو كفاءة وخبرة فنية
- 3 - تكون تلك الهجمات صرية استباقية ليكون المستهدف في موقف رد الفعل
- 4 - ويتجاوز الهجوم الالكتروني الزمان والمكان والحواجر الثقافية والتصاريس.



5 - ويعتمد على الخداع في الارتكاب والتضليل في التعرف على مرتكبيها ،

فلا تترك أثرا خلفها ، وهناك صعوبة الاحتفاظ الفنى بأثارها.

6 - تتميز دوافع الإرهاب الإلكتروني بالأساس بأنها سياسية

ويجمع الباحثون على ثلاثة دوافع اساسية للأختراق وهي: -

1. الدافع السياسي والعسكري: مما لا شك فيه أن التطور العلمي والتقني أدى إلى

الاعتماد بشكل شبه كامل على أنظمة الكمبيوتر في أغلب الاحتياجات

التقنية والمعلوماتية. فمنذ الحرب الباردة والصراع المعلوماتي والتجسسي بين

الدولتين العظميين على أشده. ومع بروز مناطق جديدة للصراع في العالم وتغير

الطبيعة المعلوماتية للأنظمة والدول ، أصبح الاعتماد كليا على الحاسب

الألي وعن طريقه أصبح الاختراق من اجل الحصول على معلومات سياسية

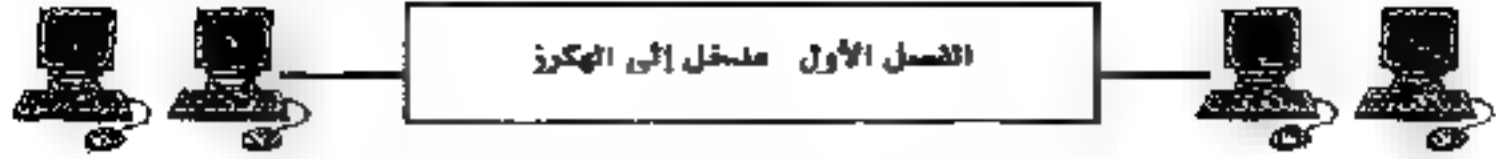
وعسكرية واقتصادية مسألة أكثر أهمية.

2. الدافع التجاري: من المعروف أن الشركات التجارية الكبرى تعيش هي أيضا

فيما بينها حربا مستمرة.

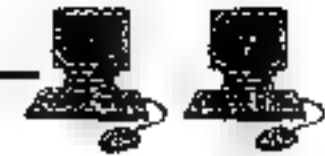
3- الدافع الفردي: بدأت في البداية ككتبا هي بين الطلاب من يستطيع اختراق

اجهزة الاخرين.



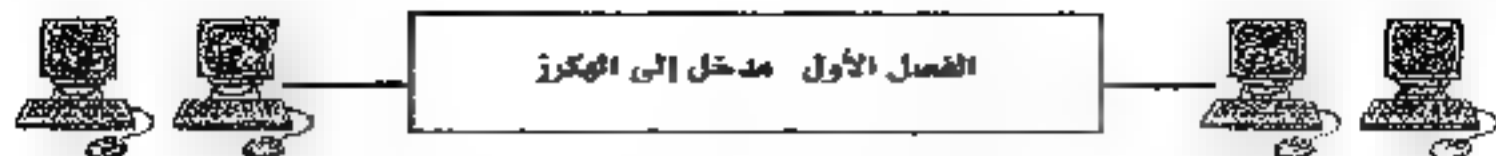
هوامش الفصل الأول:

- 1 - محمود الفريأوى . الحياة العامة و مجالات الكمبيوتر و تكنولوجيا المعلومات
هاكر , هاكلز , القراصنة , اختراق , الاختراق , الهاكرز . انظر :-
- 2 - ويكيبيديا الموسوعة الحرة انظر :
تم الاسترجاع من "http://ar.wikipedia.org/w/index".
- 3 - منتدى الحاسوب والبرامج
http://montada.echoroukonline.com/showthread.php?t=45301
- 4 - منتديات صوت القرآن 28 - 08 - 2006
/http://quran.maktoob.com/vb/quran1691
- 5 - منتديات ابن مسك .
http://benmsik.ahlamontada.com/t118-topic
- 6 - المصدر : شهاب النجار , محاضر ومدرّب لشهادة الهاكر الاخلاقي .
- 7 - المركز العربي لابعاث الفضاء الالكتروني . انظر :-
http://www.accr.co/?p=15112
- 8 _ عادل عبدالصادق . ملف الأهرام الإستراتيجي . ديسمبر 2007.
- 9 - المركز العربي لابعاث الفضاء الالكتروني انظر :-
http://www.accr.co/?p=8070
- 10 - السيد يس . جرائم الإنترنت ، دار النهضة العربية ، سنة 2000.
- 11 - إبراهيم حامد طنطاوي . الوعي التاريخي ، الثورة الكونية ، القاهرة ، سنة 1995.
- 12 - أحمد جلال عز الدين . أحكام التجريم والعقاب في قانون تنظيم الاتصالات ، دار النهضة العربية ، 2003.



- 13- أحمد سليمان الزغاليل . أساليب التعاون العربي في مجال التخطيط لمواجهة جرائم الإرهاب ، الرياض، 1414 هـ، مشار اليه في، المنشاوي، دراسة جرائم الإنترنت، www.minshawi.com.
- 14 أحمد متحي سرور . الاتجار بالنساء والأطفال، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، 1420 هـ، مشار اليه في، المنشاوي، دراسة جرائم الإنترنت www.minshawi.com.
- 15 - أحمد حسام تمام . الوسيط في قانون الإجراءات الجنائية - دار النهضة العربية، 1993.
- 16- أدور غالى النهبى الجرائم الناشئة عن استخدام الحاسب الآلى، القاهرة، دار النهضة العربية، بدون سنة نشر.
- 17- الجرائم الجنسية، بدون ناشر، 1997، الطبعة الثانية.
- 18- مجد الدين محمد بن يعقوب الفيروز . إصدار الهيئة المصرية العامة للكتاب، 1980، الجزء الرابع.
- 19- رلوف عبيد . مبادئ الإجراءات الجنائية في القانون المصري، القاهرة، دار الجيل للطباعة، الطبعة السادسة عشر، 1985، ص 358.
- 20- سمير ناجي وأشرف هلال. اداب مرافعة الادعاء "أصول وممارسات"، بدون ناشر، 2002، الطبعة الاولى.
- 21- سحر الرملاوي . السرقة والاحتيال وغسيل الاموال والاستغلال الجنسي والتجسس، سبتمبر عام 2003، مشار اليه في، www.alriadh.np.com
- 22- سعيد عبد اللطيف حسن . إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، 1999، الطبعة الأولى.
- 23 عبد الرحمن عبد العزيز الشنيقي . أمن المعلومات وجرائم الحاسب الآلى، بدون ناشر، 1414 هـ، الرياض الطبعة الأولى، مشار اليه في، المنشاوي، دراسة جرائم الإنترنت، www.minshawi.com





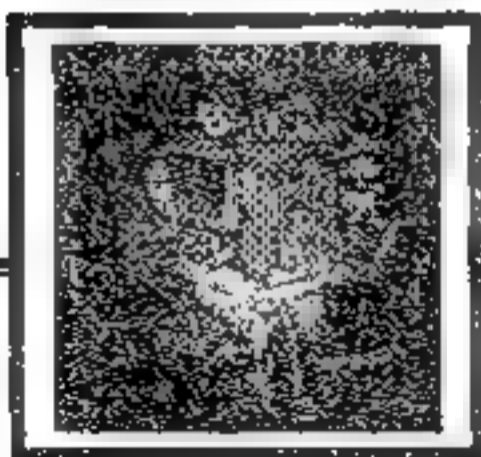
- 24- عمر الماروق الحسيني . انحراف الأحداث المشككة والمواجهة . بدون نشر ،
طبعة الثانية ، 1995.
- 25 عمر محمد يونس . الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي ،
بدون نشر ، 2005.
- 26- المجمع المعلوماتي والحكومة الإلكترونية ، اكاكوس ، 2004.
- 27- فاطمة نعناع . جريمة في فلوريدا : قضية واقعية عن استخدام شبكة الإنترنت
لتدمير حياة الآخرين ، بدون نشر ، بدون سنة نشر .
- 28 - محمود عبدالرحيم الشريفات _ " التراضي في التعاقد عبر الانترنت " _ دار
الثقافة للنشر والتوزيع _ سنة 2009.
- 29 - علاء السالمى _ " الادارة الالكترونية " _ دار وائل للنشر والتوزيع _ سنة
2008.
- 30 - نهلا المومني _ " جرائم الحاسوب " _ دار الثقافة للنشر والتوزيع _ سنة
2008.
- 31 - رياض معروزي/الجزائر. المجلة العلمية أهرام . مصر
<http://ahramag.com/modules/publisher/item.php?item.id=646>
- 32-<http://kenanaonline.com/users/ahmedkordy/posts/320929>
- 33 جروان . فتحي 2002 الإبداع ، ط 1 . الأردن ، عمان : دار الفكر للطباعة
والنشر والتوزيع.



الفصل الثاني

جرائم القرصنة

الإلكترونية





ظهرت جرائم الإنترنت مع ازدياد عمليات القرصنة وهي جرائم تختلف عن الجرائم المتعارف عليها ، فالجاني لا يحمل مسدساً ولا يسطو على متجر ، فهو جالس في بيته ولا يجد عناء في مجرد الضغط على زر يدخل به إلى شبكة الانترنت ويبدأ في اصطياذ ضحاياه، وجرائم الانترنت تعددت صورها وأشكالها فلم تعد تقتصر فقط على اختتام الشبكات وتخريبها أو سرقة معلومات منها بل شملت أيضاً جرائم أخلاقية مثل الاختطاف والابتزاز والقتل وغيرها.

وفي ظل التطورات الهائلة لتكنولوجيا المعلومات، ونظراً للعدد الهائل من الأفراد والمؤسسات الذين يرتادون هذه الشبكة، فقد أصبح من السهل ارتكاب أبشع الجرائم بحق مرتاديه سواء كانوا أفراداً أم مؤسسات أم مجتمعات محافظة بأكملها.

وتتعدد أشكال الجريمة الإلكترونية ولا يمكن حصرها، كما يولد لها كل يوم شكل جديد، وتنتشر أخبار عن حوادث وجرائم رقمية متفرقة في أنحاء المعمورة .

وهذه تسببت في تهديدات حقيقية على الأمن وأضافت أعباء جديدة إلى الشرطة المحلية المرهقة والمشغولة بالجريمة الاعتيادية، فكيف سيكون الحال وقد أضيف شكل جديد مختلف تماماً عن توأمه ويحتاج إلى خبرة ودراية وتأهيل، كما أن الجاني البسيط الذي كان يحضر إلى المدينة في السابق ليرتكب جنايته لن يضطر إلى ذلك مع الإعلام الرقمي الجديد ولعلني أطرح بعض الأشكال الخاصة بالإعلام تحديداً، وإلا فالجريمة الرقمية متشعبة وتحتاج إلى إصدار خاص بها.

وسعي بعض أصحاب المواقع الإخبارية إلى إرسال رسائل بطرق عشوائية باستخدام برامج تبث آلاف الرسائل إلى عناوين بريدية تم الاستيلاء عليها بطرق غير شرعية . مع العلم أن المواقع العالمية المالكه لمواقع البريد الإلكتروني تعد هذه الطريقة غير مشروعة وتعاقب عليها بحجب عنوان المرسل وتحويل رسائله إلى البريد غير المرغوب



كما أن هناك عمليات ملاحقة وتعقب مستمرة تقوم بها الشركات المعنية ومن ذلك ما فعلته شركة مايكروسوفت بشبكة واستوك التي كانت تقوم ببيث رسائل بريدية على بريد الهوت ميل وبكميات كبيرة جداً حيث تمكنت في النهاية من تفكيك تلك الشبكة المكونة من أكثر من مليون جهاز حاسوب.

المجرم الإلكتروني (المعلوماتي)

يعرف المجرم المعلوماتي الذي يقوم بكل هذه الجرائم الانفة الذكر حيث يختلف الكثير في تعريفه وتحديد هويته وتقدير مدى عقوبته ولكن يمكن تلخيص سماته بأنه مجرم متخصص؛ له قدرة عالية في المهارات الحاسوبية والتقنية ويستغل هذه المهارات في اختراق نظم التشغيل واكتشاف كلمات المرور أو الشفريات ليحصل على المعلومات الموجودة على أجهزة الحواسيب ومن ثم يقوم بتخزينها للاستفادة منها وكذلك السرقة والنصب والاعتداء على حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال ، كما أنه يقوم باخفاء أي اثر له لكي لا تكتشفه الأنظمة الأمنية حتى لا تستطيع مراقبته أو ملاحقته من خلال أي شبكة .

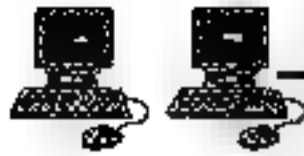
الجريمة الإلكترونية

تعددت المسميات التي أطلقت على الجرائم الإلكترونية، فالبعض أطلق عليها الجرائم الاقتصادية المرتبطة بالكمبيوتر Computer-Related Economic Crime، وهي تشير إلى الجرائم التي تستهدف قطاعات الأعمال، أو تلك التي تستهدف السرية وسلامة المحتوى وتوفر المعلومات.

و من الملاحظ على المسمي السابق أنه لا يعبر عن كافة أشكال الجرائم، و لكنه اقتصر على نوع واحد من تلك الجرائم، و هو الجرائم الاقتصادية.

وهناك من أطلق عليها اصطلاح جرائم أصحاب الياقات البيضاء، White Collar Crime، والتي تشير إلى الجرائم التي ترتكب من قبل أشخاص لهم مكانة عالية في المجتمع، وذلك من خلال قيامهم بأعمالهم المهنية، فجرائم





أصحاب الياقات البيضاء هي جرائم طبقة اجتماعية تستغل وضعها الطبقي في الحصول على منفعة شخصية بوسائل غير قانونية، ليس من السهل اكتشافها من قبل السلطات المختصة؛ نظرا لوضع هذه الطبقة والإمكانيات المتوفرة لديها لإخفاء جرائمها.

وهذا المسمى للجرائم الإلكترونية لا يوضح بدقة طبيعة هذه الجرائم من حيث أدواتها ووسائلها؛ حيث إنه لم يشر إلى الكمبيوتر أو أية تقنية أخرى كأداة أو هدف للجريمة، ولكن هذا التعريف اتسم بالعمومية؛ إذ أشار إلى نوع من الجرائم قد ينطبق أيضا على الجرائم التقليدية.

والبعض أطلق عليها Crime Cyber؛ على اعتبار أن هذا الاصطلاح شامل لجرائم الكمبيوتر وجرائم الشبكات، كما أن كلمة Cyber تستخدم لدى الأكثرية بمعنى شبكة الإنترنت ذاتها أو العالم الافتراضي، في حين أنها أخذت معنى عالم أو عصر الكمبيوتر بالنسبة لبعض الباحثين. كما أطلق عليها البعض الجرائم المتعلقة بالكمبيوتر Computer-Related Crimes، وهي تلك الجرائم التي يكون الكمبيوتر فيها وسيلة لارتكاب الجريمة، كالاختيال بواسطة الكمبيوتر والتزوير ونحوهما. وهناك من أطلق عليها Computer Crimes أي جرائم الكمبيوتر؛ للدلالة على الأفعال التي يكون الكمبيوتر فيها هدفا للجريمة، كالدخول غير المصرح به، أو إتلاف البيانات المخزنة في النظم ونحو ذلك. كما عرفها البعض بأنها "نشاط موجه ضد أو المنطوي على استخدام نظم الحاسوب، والتعريفان السابقان يركزان على دور الكمبيوتر كأداة أو هدف للجريمة.

كما تعرف بأنها "آية جريمة أفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها" والتعريف السابق يشير إلى سمة من سمات مرتكب هذا النوع من الجرائم، وهي المعرفة الفنية بالحاسب الآلي، وبالتالي فهو يركز على مرتكب الجريمة أكثر من تركيزه على الهدف منها أو أشكالها.



كما تعرف بأنها كل نشاط يتم فيه استخدام الكمبيوتر كأداة أو هدف أو وسيلة للجريمة. ويشير التعريف السابق إلى الأدوار المتنوعة للكمبيوتر في ارتكاب مثل هذه الجرائم .

و لكن الملاحظ علي جميع التعريفات السابقة أنها لم تشر إلا إلى الكمبيوتر، أيا كان دوره في ارتكاب مثل هذه الجرائم ، ولكنها لم تشر إلى أية تقنية أخرى، من هنا فإن البحث الحالي يرى أنه على الرغم من أن الكمبيوتر يلعب دورا هاما جدا في ارتكاب مثل هذه الجرائم ، فإن هذه الجرائم لا تقتصر فقط علي الكمبيوتر، بل تشمل أية تقنية أخرى يمكن أن تستخدم في ارتكابها كالتلف النقال على سبيل المثال.

والجرائم الإلكترونية بهذا المعنى تشير في إحدى تعريفاتها إلى "أنها كل نشاط أو سلوك غير مشروع أو غير مسموح به ، فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات".

ويعتمد هذا التعريف على معيارين: أولهما وصف السلوك بأنه غير مشروع، وثانيهما اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها ، وهو بذلك تعريف جامع لكل التقنيات التي تحدث فيها المعالجة الآلية للبيانات ، دون الاقتصار على الكمبيوتر.

كما تعرف بأنها "أي فعل ضار يقوم به الفرد عبر استعماله الوسائط الإلكترونية مثل الحواسيب، و أجهزة الموبايل، و شبكات الاتصالات الهاتفية، و شبكات نقل المعلومات، و شبكة الإنترنت، أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الإلكترونية".

والجريمة الإلكترونية لها مسميات عدة منها :

- 1- جرائم الحاسوب والإنترنت
- 2- جرائم التقنية العالية
- 3- الجريمة الإلكترونية
- 4- الجريمة السليبرية





5- جرائم أصحاب الياقات البيضاء.

منفذو الجريمة الإلكترونية :

تتنوع أعمار منفذي الجرائم الإلكترونية مع اختلاف دوافعهم . فهناك من سفدي الهجمات الأطفال والمراهقين الذين تكون في الغالب دوافعهم لمجرد التسلية غير مدركين حجم الأضرار التي يقومون بها ، وهناك المحترفين والمختصين والإرهابيين الذين من الممكن ان تحطم أعمالهم شركات ضخمة وتضر بدول كبيرة .

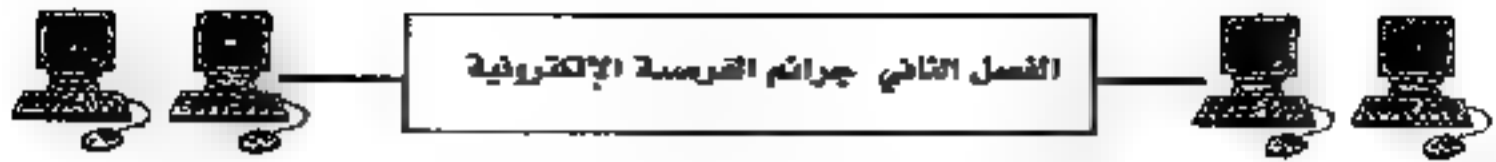
أهداف الجرائم الإلكترونية :

- نستطيع تلخيص بعض أهداف الجرائم الإلكترونية ببضعة نقاط أهمها .
- 1- التمكن من الوصول الى المعلومات بشكل غير شرعي ، كسرقة المعلومات او الاطلاع عليها او حذفها او تعديلها بما يحقق هدف المجرم.
 - 2- التمكن من الوصول عن طريق الشبكة العنكبوتية إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها
 - 3- الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالمؤسسات والبنوك والجهات الحكومية والأفراد وابتزازهم بواسطتها .
 - 4- الكسب المادي أو المعنوي أو السياسي غير المشروع عن طريق تقنية المعلومات مثل عمليات اختراق وهدم المواقع على الشبكة العنكبوتية وتزوير بطاقات الائتمان وسرقة الحسابات المصرفية ، الخ ...

وهناك أنواع الجرائم الإلكترونية تبعاً لـ:

- 1- لدور الحاسب في الجريمة:
- أ الحرائم التي تستهدف عناصر (السرية والسلامة) وتضم:
- الدخول غير الشرعي
 - الاعتراض غير القانوني.





- تدمير البيانات بمسحها أو تعطيلها أو تشويبها وجعلها غير قابلة للاستخدام
- إساءة استخدام الأجهزة

ب. الجرائم المرتبطة بالحاسب وتضم :

- التزوير

- الاحتيال

- قرصنة البرمجيات : كالاخلاق بحقوق المؤلفين

2 - تبعاً لمساسها بالأشخاص والأموال:

أ. جرائم التي تستهدف الأشخاص : تستهدف الأشخاص ومن الممكن أن يصل إلى قتل الأشخاص بالحاسوب .

ب. جرائم الأموال: التي تستهدف الملكيات الشخصية متضمنة إتلافها بدون سرقتها .

ج. جرائم الاحتيال والسرقة: ويشمل ذلك كل من سرقة الممتلكات الشخصية والمعلومات الإلكترونية المخزنة في الأجهزة .

د. جرائم التبدل والتزوير: وذلك بتبديل المعلومات المخزنة على الأجهزة وتغييرها أو التقاط الرسائل المرسلة بين الأجهزة وتحريفها .

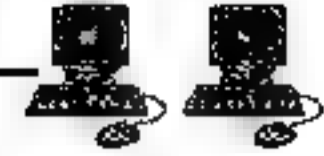
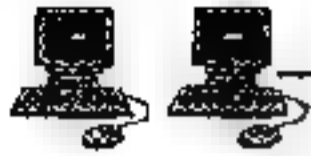
مراحل تطور الجرائم الإلكترونية

1- الجرائم التقليدية الإلكترونية

تتعدد هذه الجرائم، وبالنظر إلى كونها ترتكب باستخدام وسائل تقنية، فإننا سوف نقصر حديثنا على جريمة الاستيلاء على الأموال عن طريق الاحتيال. (التحويل الإلكتروني غير المشروع للأموال). وفيما يتلاعب الحاني في البيانات المخزنة في ذاكرة الحاسب الآلي أو في برامجه وفقاً لأساليب متعددة، بهدف تحويل كل أو بعض أرصدة الغير أو فوائدها إلى حسابه.

فالنصب هو الاستيلاء بطريق الاحتيال على شيء مملوك للغير سية تملكه .

وقد اختلفت لتصوص القانونية في دول العالم كافة في معاقبة هكذا جريمة



فعلى سبيل المثال نص قانون العقوبات المصري في المادة 336 على أن يعاقب بالحبس كل من توصل إلى الاستيلاء على نقود أو عروض أو سندات دين أو سندات مخالصة أو أي متاع منقول وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها إما باستعمال طرق احتيالية من شأنها إيهام الناس بوجود مشروع كاذب أو واقعة مرورة أو أحداث الأمل بحصول ربح وهمي أو تسديد المبلغ الذي أخذ بطريق الاحتيال أو إيهامهم بوجود سند دين صحيح أو سند مخالصة مزور وإما بالتصرف في مال ثابت أو منقول ليس ملكاً له ولا له حق التصرف فيه، وإما باتخاذ اسم كاذب أو صفة غير صحيحة.

ويتكون الركن المادي في جريمة النصب من فعل الاحتيال أولاً، ومن استيلاء الجاني على منقول مملوك للغير ثانياً، ومن علاقة سببية بين الأمرين أخيراً، أما الركن المعنوي فيتميز باشتعاله على قصد خاص بجانب القصد العام. وتتركز المشكلات التي يثيرها الفقه بخصوص هذه الجريمة في أمرين: - أولهما: مدى جواز الاحتيال على نظام الحاسب الآلي وإيقاعه في الغلط. وثانيهما: مدى اعتبار النقود الكتابية أو البنكية من قبيل الأموال المادية التي يرد عليها الاستيلاء.

أولاً: الاحتيال على نظام الحاسب الآلي

الاحتيال هو كل نظام أو إيهام يكون صالحاً لإيقاع لمجني عليه في الغلط بطريقة تؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي، أي أن المجني عليه في جريمة النصب هو من جازت عليه حيلة الجاني فانخدع بها وسلمه ماله وتباينت اتجاهات التشريعات المقارنة في شأن الإجابة عن تساؤل محله هل يمكن ممارسة أفعال الاحتيال على الحاسب الآلي وإيقاعه في الغلط؟ الاتجاه الأول:

ويستلزم لتوافر جريمة النصب أن يكون الجاني قد خدع إنساناً مثله، وأن يكون الإنسان المخدوع مكلفاً بمراقبة البيانات. ومن ثم لا يتصور وفقاً لهذا الاتجاه



خداع الحاسب الآلي بوصفه آلة ، ولا يجوز تطبيق النص الجنائي الخاص بالنصب لافتقاده لأحد العناصر اللازمة. ويتبنى هذا الاتجاه كل من مصر وألمانيا وإيطاليا والتشريع الفرنسي وإن صيغ على نمط هذه التشريعات، إلا أن هناك اتجاهاً في الفقه الفرنسي يرى أن خداع الحاسب الآلي لمسلب مال الغير يتحقق به بالطرق الاحتمالية ككذب تدعيمه أعمال مالية أو وقائع خارجية، حيث يتوافر فيه بالإضافة إلى الكذب، واقعة خارجية تسانده هي إبراز أو تقديم المستندات أو المعلومات التي تدخل إلى الحاسب.

الاتجاه الثاني:

وتمثله تشريعات دول الأنجلوسكسون والتي جاءت نصوصها في مجال النصب على نحو أعم وأشمل من نظيرتها الأوروبية، وبحيث يمكن تطبيقها على النصب المعلوماتي.

وتأخذ بهذا الاتجاه إنجلترا وكندا وأستراليا.

الاتجاه الثالث:

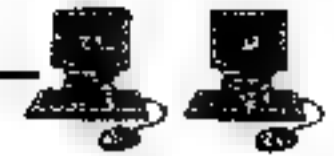
وتمثله الولايات المتحدة، حيث يطبق هناك القوانين الخاصة بالفسح في مجال البنوك والبريد والتلغراف، والإتفاق الإجرامي لأغراض ارتكاب الفسح، على حالات النصب المعلوماتي.

تستهدف التشريعات التي أمدت نطاق تطبيق نصوص في مجال النصب على النصب المعلوماتي، الحد من جرائم التلاعب في البيانات المعالجة إلكترونياً بواسطة الحاسبة الآلي.

ثانياً: الاستيلاء على نقود كتابية أو بنكية

ر نشاط الجاني في جريمة النصب مركب لا بسيط، فهو يتكون من فعلين مختلفين، هما الاحتيال والاستيلاء. وأول الفعلين يتقدم الثاني في الزمن ويفصي إليه بحكم المنطق، ومحل الاستيلاء في جريمة النصب هو المال المنقول والذي حدده المشرع المصري في المادة 336 عقوبات بأنه "نقود أو عروض أو سندات





دين أو سندات مخالصة أو متاع منقول " ويتحقق الاستيلاء على المال في هذه الجريمة بتسليم المجني عليه المال بمحض إختياره إلى الجاني تحت تأثير الغلط الذي أوقعه فيه فعل الاحتيال.

ولا يرتب الإستيلاء الناشئ عن الاحتيال على الحاسب الآلي أدنى مشكلة إذ، كان محل الاستيلاء نقوداً أو أي منقول آخر له قيمة مادية، كأن يتم لتلاعب في البيانات الداخلة أو المخزنة بالحاسب أو برامجه، بواسطة شخص ما كي يستخرج الحاسب بإسمه أو بإسم شركائه، شيكات أو فواتير بمبالغ غير مستحقة يستولي عليه الجاني أو يتقاسمها مع شركائه.

وأهمية الأمر عندما يكون محل هذا الاستيلاء نقوداً كتابية أو بنكية، أي أن في هذا الفرض يتم الاستيلاء على المال عن طريق القيد الكتابي، وصورة ذلك أن يتلاعب شخص في البيانات المخزنة في الحاسب كي يحول بعض أرصدة الغير أو فوائدها إلى حسابه .

إنجاء عدد محدود من الدول، كما هو الحال في كندا وهولندا وسويسرا وإنجلترا ومعظم الولايات المتحدة الأمريكية إلى اعتبار النقود الكتابية - وعلى الرغم من طابعها غير المحسوس - من قبيل الأموال التي تصلح لأن تكون محلاً لجرائم السرقة والنصب وخيانة الأمانة .

وعلى النقيض ذهب بعض التشريعات - كما هو الحال في ألمانيا واليابان - إلى عدم اعتبار النقود الكتابية بمثابة مال مادي، ولكن ينظر إليها بوصفها من قبيل الديون والتي يستحيل أن تكون محلاً للاختلاس أو السرقة.

أما التشريع الفرنسي فإن القضاء الفرنسي إبتدع نظرية التسليم المعادل، ومؤداها أن مجرد القيد الكتابي والذي لا يقتضي تسليم شيء مادي أياً كان، يعد من قبيل التسليم المعادل. وتلقف الفقه الفرنسي نظرية التسليم المعادل التي أرسنها محكمة النقض الفرنسية. وقام بتطبيقها على جميع أفعال التلاعب في عملية البرمجة، أو في البيانات المدخلة إلى الحاسب الآلي، والتي تؤدي إلى إلغاء رصيد دائن، أو من باب أولى خلق رصيد دائن بمبالغ غير مستحقة





وتتعدد الأساليب المستخدمة في هذا الشأن، فقد يحدث ذلك عن طريق إلتقاط أمر التحويل بواسطة الجاني، أو تزيفه بالأمر بتحويل نقص المبلغ بحسابه الخاص، أو عن طريق التلاعب في عملية البرمجة بفرض تحويل فواتر حساب شخص ما إلى حساب الفاعل، وأخيراً عن طريق انتحال الفاعل لشخصية الغير ومباشرة لعملية تحويل النقود. وبالتالي فإن الدفع يتم بمجرد القيد الكتابي، وهو يعادل تسليم النقود.

2 - الجرائم المستحدثة في مجال المعلوماتية

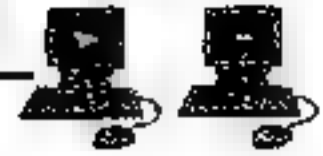
أدى ربط الحاسبات الآلية بعضها ببعض عن طريق شبكات المعلومات إلى سرعة انتقال المعلومات من جهة، وإلى سهولة التطفل عليها من جهة أخرى عن طريق استخدام "المودم" حيث يسمح هذا الجهاز للمتطفلين من أي مسافة بتواجدون فيها بالولوج إلى الحاسبات الآلية المستهدفة، ودون أي مساس مادي بحق ملكية الغير أو ترك أي أثر يدل على إنتهاك المعلومات أو نسخها .

ونظراً لجسامة هذا النوع من التعدي، فقد حرصت دول كثيرة على إرساء مبدأ حماية سلامة نظم المعلومات لديها وبفض النظر عن مبدأ حماية سرية البيانات المعالجة أو المتداولة.

وبالرغم من أهمية هذه الحماية، فإن ثمة صعوبات في تطبيق النصوص التقليدية. ذلك أن غائية الأنظمة القانونية لا تستهدف النصوص التقليدية التي تجرم التصنت على المكالمات التليفونية والتقاط المراسلات المتبادلة، سوى تسجيل المحادثات أو الإتصالات الشفوية أي التي تتم بين شخصين فأكثر.

وعلى سبيل المثال أن المادة 716 المستحدثة من قانون العقوبات الإيطالي يقتصر تطبيقها على الاتصالات التي تجري بين شخصين، وهذا هو الحال أيضاً من القوانين العقابية الألمانية والسويسرية والهولندية والمصرية. وأيضاً في الولايات المتحدة حيث يستهدف القانون الفيدرالي الخاص بمراقبة المكالمات التليفونية الصادر سنة 1968 الإتصالات الشفوية التي تتم بواسطة أنظمة الإتصالات البعيدة، ودون أن يستطيل ذلك إلى البيانات المتدفقة بين الحاسبات الآلية .





بينما يذهب قانون العقوبات الكندي عكس ذلك، حيث تجرم المادة 178 منه التقاط المراسلات التي تتم بين الحاسبات الآلية، ولكن بشرط أن يكون هناك اتصال شفوي بين شخصين أو عن طريق أنظمة الاتصالات البعيدة، ومن ثم لا تسري هذه المادة على الاتصالات التي تجري بين حاسبين آليين يخصصان شخص واحد، أو على الاتصالات التي تجري بين حاسبين آليين، أو على الاتصالات المتبادلة داخل نظم معلوماتي واحد.

والعقوبات التي تثار عند تطبيق النصوص الجنائية التقيدية على الأنماط المستحدثة لظاهرة الغش المعلوماتي ما زالت أكثر وضوحاً في مجال "مجرد" الولوج غير المسموح به في أنظمة معالجة وتخزين البيانات تعني مجرد "الولوج غير المسموح به في حاسب آلي، فعل التواجد به بدون إحداث أدنى ضرر لمصاحبه، سوى لإطلاع على المعلومات المخزنة به وبدون غرض محدد .

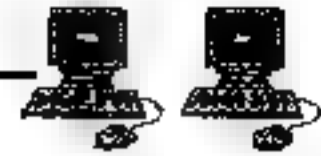
أما عن الحلول التشريعية، فإن المشكلة في هذا المجال هي معرفة ما إذا كان يجب تنظيم الولوج في المعلومات والبيانات، أم يجب حماية المعلومات لذاتها، أو أن يعمل بالحالين معاً في نفس الوقت، على اعتبار أن التعدي على البيانات والمعلومات وما يتحقق من لحظة التعدي - على النظام المعلوماتي.

بيد أن المشكلة الأكثر جسامة هي معرفة ما إذا كان من الملائم تجريم مجرد الوجود في الأنظمة، أم يجب أن يقتصر هذا الأخير بأفعال أخرى كتعديل معلومات أو حيزتها أو إستخدامها أو إحداث ضرر بها.

اتجهت بعض الدول إلى النص في تشريعاتها على تجريم فعل الولوج في المعلومات أو البرامج المخزنة في أجهزة المعالجة الإلكترونية للمعلومات، ومن هذه الدول السويد والدنمارك .

أما الولايات المتحدة، فإن التشريع الفيدرالي الصادر سنة 1984 يحذر الولوج بدون نصريح في الحاسبات الآلية المستخدمة من قبل الحكومة الفيدرالية والبنوك .





أما التشريع الفرنسي، فإن القانون الفرنسي الصادر في 5 يناير 1988 استحدث بموجب المادة 2/462 عقوبات، جريمة الولوج غير المشروع في نظم المعلومات والتي تنص على أن يعاقب.....كل من وُلج أو تواجد بطريق الغش في كل أو جزء من نظام مبرمج للبيانات. وتشدّد العقوبة إذا ما ترتب على ذلك إلغاء أو تعديل للبيانات التي يحتويها النظام أو إتلاف لوظيفة هذا النظام.

ويستهدف هذا النص في المقام الأول - حماية الولوج في نظم المعلومات، لا حماية حق الملكية ذاته، وهو بذلك فراغاً تشريعياً هائلاً في القانون الفرنسي، ومن جهة أخرى استجابة لرغبة ملاك الأنظمة المعلوماتية.

اسباب جرائم القرصنة الالكترونية

يختلف مرتكبو جرائم المعلوماتية عن مرتكبي الجرائم الاعتيادية من حيث المبدأ وطريقة القيام بالعمل الحرامي، لكن بالنهاية يبقى الطرفان مخالفين للقانون، لذا يستحقون العقاب بما اقترفوا من جرائم.

وهناك عدة أسباب تدفع لارتكاب الجرائم المعلوماتية يمكن أن نوجزها

بالآتي:

1 - حب التعلم

يعتبر حب التعلم والاستطلاع من الأسباب الرئيسة التي تدفع لارتكاب مثل هكذا جرائم لأن المخترق يعتقد أن أجهزة الحاسوب والأنظمة هي ملك للجميع ويجب أن لا تبقى المعلومات حكرًا على أحد أي أن للجميع الحق بالتعرف والاستفادة من هذه المعلومات.

2 - المنفعة المادية

قد تكون محاولات الكسب السريع وجني الأرباح الطائلة دون تعب ولا رأس مال من الأسباب التي تدفع لاختراق أنظمة الكمبيوتر كالتّي تستخدمها المصارف عن طريق الدخول إلى الحسابات المصرفية والتلاعب فيها أو الاستخدام غير المشروع لبطاقات الائتمان.





3 - التسلية واللهو

عدد غير قليل من مخترقي الأنظمة يعتبرون أن عملهم هذا وسيلة للمرح والتسلية وتقضية اكبر وقت ممكن في أنظمة وحواسيب الآخرين ويكون هذا الاختراق غالباً سلبياً ودون أن يحدث تأثير يذكر.

4 - الدوافع الشخصية

يعتبر محيط الإنسان والبيئة التي يعيش فيها من العوامل المؤثرة في سلوكه وتصرفاته وغالباً ما تدفع مشاكل العمل إلى رغبة بالانتقام ووجود أنظمة الكترونية تسهل له القيام برغباته فيعيب بمحتوياتها إلى درجة التخريب ، أو يكون الدافع التحدي وإثبات الجدارة أمام الآخرين بحيث يفتخر هذا الشخص بأن باستطاعته اختراق أي حاسوب أو أي نظام ولا يستطيع احد الوقوف بوجهه.

وقد تكون هناك اسباب ودوافع اخرى منها :-

- 1 - غياب الامانه لدى موردين ومنتجين البرامج المقلدة والمفشوشة .
- 2 - التحدي والتفوق على النظام الالكتروني وإثبات القدرات الفنية .
- 3 - الرغبة في الانتقام من فرد أو منظمه كالايتزاز والتشهير .
- 4 - التنافس الايديولوجي بين الدول ومناهضة المولة .
- 5 - صعوبة التحقيق والتحريات وعدم إثبات الأدلة وضعف المقننات الصادرة بحق مجرمي المعلومات .

ويتركز عمل القراصنة عادة على:

- إيجاد أرقام الهواتف الهامة التي ترتبط بها الأنظمة الكمبيوترية المستهدفة.
- اكتشاف أنظمة الموديم التي تربط أنظمة الكمبيوتر بالشبكة الهاتفية ونقاط الوصول إلى الشبكات الكمبيوترية.
- الحصول على البيانات المخزنة في أجهزة كمبيوترية غير مرتبطة بشبكات عن طريق التقاء الموجات الكهرومغناطيسية المنبعثة عن هذه الأجهزة عند تشغيلها .



أنواع الجرائم الإلكترونية

ويمكن تقسيمها الى:

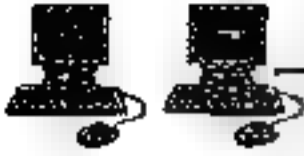
1 - الجرائم الاقتصادية

تتنوع الجرائم الاقتصادية بتنوع النظام السائد في الدولة فعلى سبيل المثال في الدول الرأسمالية نجد ان اغلب الجرائم الاقتصادية تتمحور حول الاحتكارات والتهرب الضريبي والجمركي والمطو على المصارف وتجارة الرقيق الابيض والاطفال، في حين تتمحور تلك الجرائم في النظام الاشتراكي على الرشوة والاختلاس والسوق السوداء. وهذا لا يعنى بالضرورة انه لايمكن ارتكاب كل انواع هذه الجرائم في مجتمع واحد حيث يمكن ان تجد في المجتمع الرأسمالي مثلاً جرائم رشوة واختلاسات والعكس صحيح.

وكما في الجرائم الأخرى فان الإنترنت ساهم في تطوير طرق واساليب ارتكاب هذه الجرائم وتوسيع منطقة عملها خاصة مع توجه الكثير من الدول في التحول إلى الحكومات الاللكترونية كما في دولة الامارات العربية المتحدة مثلاً، حيث استفاد المجرمون من التقدم التقني في اختلاس الاموال وتحويل الارصدة النقدية وكذلك في سرقة التيار الكهربائي والمياه وخطوط الهاتف والعبث بها واتلافها.

ويندرج تحت هذا البند حادثة اقتحام متسللين لنظام الحاسب الآلي الذي يتحكم في تدفق اغلب الكهرباء في مختلف انحاء ولاية كاليفورنيا الامريكية، وسال رغم من ان الهجوم كان محدوداً الا انه كشف عن ثغرات أمنية في نظام الحاسب الآلي لشركة الكهرباء .

وتتعدد الآثار السلبية لهذا النوع من الجرائم ، فمن الناحية الاقتصادية تكلف الدول أموالاً طائلة ؛ حيث قدرت الخسارة العالمية الناجمة عن تلك الجرائم عام 2007 بنحو 200 مليار، وتقدر خسائر الأمريكيين وحدهم بحوالي 240 مليون دولار⁽²⁾ .



أما على المستوى المحلي فتشير الإحصائيات إلى أن حجم القرصنة في مصر وصل حوالي 65 / عام 2007، و أنه قد أدى إلى خسارة الدولة 50 مليون دولار في هذا العام .

وتتمثل انعكاسات الجريمة الإلكترونية على الاقتصاد العالمي بـ : -
أ. الخسارة المالية بسبب الابتزاز:

تمت في مصر عملية ابتزاز عن طريق الشبكة العنكبوتية و ذلك بتهديد شركة مياه غازية بنشر صورة لأحد منتجاتها و بداخلها حشرة، ولكن لم ترضخ الشركة إلى التهديد و نشر المبتزون الصورة و شاهدا 3700 شخص و تم التعرف على المبتزين و اعترفوا بجرمهم.

ب. الخسارة المالية بسبب بعض الموظفين المطرودين:

تيموثي ألن ليود هو مصمم ومبرمج فصل من عمله، فما كان منه إلا أن أطلق قبيلة إلكترونية ألقت كافة التصاميم وبرامج الإنتاج لأحد أكبر مصانع التقنية العالية في نيوجيرسي التي تعمل لحساب وكالة الفضاء NASA والبحرية الأمريكية.

ج. الخسارة المالية بسبب سرقة المعلومات الشخصية:

- في بنك لويدز في أمستردام تم تحويل مبلغ 8.4 مليون دولار إلى بنك في سويسرا من قبل شاب عمره 26 عام.

- في عام 2000م ، جرى السطو على 33 ألف جهاز صرف الي ATM في بريطانيا ، و قد كانت الخسارة المالية كبيرة قدرت بنحو 15 مليون جنيه إسترليني.

ولا يزال هناك قلق عالمي كبير على المستوى الأمني والاقتصادي والإداري نتيجة الاحتراقات الإلكترونية المتعددة التي تشهدها المنشآت مما جعل من أمن المعلومات هاجسا لدى الدول والشعوب والمنظمات والشركات والمنشآت الاقتصادية وذلك على كافة المستويات الأمنية والإدارية والاقتصادية .





وطالب خبراء اقتصاديون ومختصون في أمن المعلومات بضرورة تطبيق معايير عالمية في مجال حماية المعلومات في كافة المنشآت الوطنية خاصة البنوك والمنشآت التي يحتم عليها حفظ معلومات ضخمة سواء للأفراد أو المنشآت .

في ظل ما تطألفنا به الأخبار من فترة لأخرى لاختراقات حدثت لشبكات معلومات عالمية مهمة أو لقرصنة المعلومات من مواقع العديد من الجهات ومنها ما نشر عن قرصنة المعلومات لموقع البنتاجون مما يستدعي الاهتمام بأمن المعلومات والبحث عن الوسائل والبرامج الكفيلة بحماية معلومات منشآتنا الوطنية المختلفة .

وفي هذا الإطار يشير خبراء ومختصون في الأمن المعلوماتي إلى أن الاختراقات والقرصنة الإلكترونية تهدد العديد من المنشآت المحلية المهمة، كما أن العديد من الحقائق المرتبطة بمجال تقنية المعلومات وسهولة الاتصالات على مستوى العالم نتج عنه العديد من الحقائق منها أن هناك ملياري مستخدم للإنترنت حول العالم وأن وسائل التواصل الاجتماعي هي النشاط الأول على شبكة الإنترنت الآن . ويأتي افتقار معظم الشركات والمنشآت الوطنية لتطبيق مفهوم السياسات الأمنية للمعلومات وذلك لعدم وعيها بفوائد تلك السياسات التي من شأنها أن تقلل من المخاطر الأمنية التي تتعرض لها .

وعليه بات من الضروري تحفيز المنشآت الوطنية لتبني المعايير والسياسات الأمنية العالمية والتي تهتم بتأمين البيانات التي تخص المنشآت والمستفيدين منها ورفع المستوى الأمني بشكل عام في جميع تعاملات المنشآت الإلكترونية من الأمن المادي إلى الأمن الإلكتروني .

ويطالب الخبراء في هذا المجال بأهمية قيام الجهات المختلفة بتطبيق وتبني المنشآت للبرامج المساعدة في حفظ البيانات والمعلومات الخاصة بها وحمايتها من أي اختراقات أو قرصنة قد تتعرض لها حتى لا تتأثر هذه المنشآت بهذه الاختراقات والتي تساعد المتعاملين مع هذه المنشآت وتغرس في نفوسهم الثقة تجاه مثل هذه المنشآت نتيجة لاستخدامها برامج حماية لكافة تعاملاتها .





وهناك جريمة تزوير البيانات التي تنطوي تحت طائلة الجرائم الاقتصادية وتتم عمية التزوير بالدخول إلى قاعدة البيانات وتعديل البيانات الموجودة بها أو اضافة معلومات مغلوطة بهدف الاستفادة غير المشروعة من ذلك.

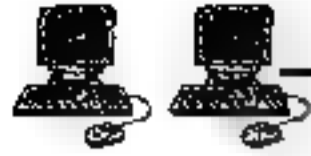
وقد وقعت حادثة في ولاية كاليفورنيا الامريكية حيث عمدت مدخلة البيانات بنادي السيارات وبناء لاتفاقية مسبقة بتغيير ملكية السيارات المسجلة في الحاسب الآلي بحث تصبح باسم احد لصووس السيارات والذي يعمد إلى سرقة السيارة وبيعها وعندما يتقدم مالك السيارة للإبلاغ يتضح عدم وجود سجلات للسيارة باسمه وبعد بيع السيارة تقوم تلك الفتاة باعادة تسجيل السيارة باسم مالكها وكانت تقاضى مقابل ذلك مبلغ مائة دولار.

وفي حادثة اخرى قام مشرف تشغيل الحاسب باحد البنوك الامريكية بعملية تزوير حسابات اصدقائه في البنك بحيث تزيد ارصدتهم ومن ثم يتم سحب تلك المبالغ من قبل اصدقائه وقد نجح في ذلك وكان ينوى التوقف قبل موعد المراجعة الدورية لحسابات البنك الا ان طمع اصدقائه اجبره على الاستمرار إلى ان قبض عليه.

ويتوقع باحثون ودارسون في مجال الالكترونيات الى ازدياد فرص ارتكاب مثل هذه الجرائم مع التحول التدريجي الى الحكومات الالكترونية حيث سترتبط الكثير من الشركات والبنوك بالإنترنت مما يسهل الدخول على تلك الانظمة من قبل محترفي اختراق الانظمة وتزوير البيانات لخدمة اهدافهم الاجرامية .

2- الجرائم الأخلاقية

ذكرت وكالة "أنثارا" الإندونيسية الحكومية للأنباء مؤخراً أن بلدة جونوج كيدول في إقليم يوجياكارتا على جزيرة جاوة الوسطى، شهدت زيادة حادة في عدد الراغبين في الحصول على تصاريح زواج خلال العامين الماضيين، وبقلت الوكالة عن سيتي هاريانتي، الأمنية في محكمة شرعية في جونونج كيدول،



القول، "كثيراً ما سألنا القاصرين ما إذا كان التعارف بينهم قد تم عبر الفيسبوك، وأقروا بذلك .

وأضافوا أنهم استمروا في العلاقة إلى أن أصبحت الفتاة حاملاً ، وقالت هاريانتي إن "الدخول على الفيسبوك بات سهلاً ، حتى في القرى ، ما يؤدي إلى أن تصبح المتيات حوامل خارج نطاق الزواج" ، وقالت هاريانتي ، إن 130 شاباً وفتاة تتراوح أعمارهم بين 16 و 19 عاماً سمعوا هذا العام إلى الحصول على تصاريح زواج من المحكمة الشرعية - وهو ما يزيد بنسبة 100% عن العام الماضي ، وبموجب القانون الإندونيسي فإن السن القانونية للزواج هي 16 عاماً للفتاة و 19 عاماً للشباب ، وبلغ عدد مستخدمي الفيسبوك في إندونيسيا 35 مليون شخص ، ما يجعلها ثاني أكبر سوق لاستخدام الموقع بعد الولايات المتحدة ، حسب موقع "جلوبال بوست" الأمريكي على الانترنت.

3 - الجرائم الاجتماعية

تطالعنا المواقع الاجتماعية يومياً بقصص وروايات عن جرائم اجتماعية يقع صاحبها مستخدمي شبكة المعلومات الدولية ولاسباب واهداف شتى . ففي مدينة ماونت فيو الصغيرة في ولاية تينيسي (جنوب الولايات المتحدة) انتهى خلاف نشب على "فيسبوك" بجريمة قتل الزوجين الشابين حسبما أعلنت الشرطة المحلية في المدينة والتي اعتقلت المشتبه بهما . وقتل بيلى كلاي باين (36 عاماً) وبيلى جين هيوورث (23 عاماً) في 31 كانون الأول /ديسمبر برصاصات عدة في الرأس . وتم أيضاً ذبح باين فيما عثر على ابنهما حياً بين دراعي والدته ، على ما أوضح الشريف مايك ريس لوكالة فرانس برس .

واعتقلت الشرطة مشتبهاً بهما اثنين ووجهت إليهما تهماً بالقتل ووضعتهما رهن الاعتقال.





واظهر التحقيق أن المشتبه بهما كانا الضحيتان قد رفعوا شكوى ضدهما السنة الماضية بتهمة الازعاج والتهديد عبر الهاتف والانترنت.

وشرح أن المرأة الثلاثينية تعاني إعاقة جسدية وتقضي معظم وقتها على "فيسبوك" لكنها استشاطت غيظا بعدما قرر الكثيرون قطع علاقتهم بها على موقع التواصل الاجتماعي بمعوها من لائحة "الأصدقاء".

وأضاف لدى القضاء قضايا ازعاج ومضايقة عدة بشأن هذه المرأة على فيسبوك لكن الأمور خرجت عن السيطرة هذه المرة. إنه السبب الوحيد الذي يمكننا تقديمه لتفسير دوافع الجريمة.

وتابع "لكني لا أعرف لم اختار (القاتلان) هذين الشاب والشابة بالتحديد من بين كل الأشخاص الذين كانت لديهما مشاكل معهم".

وأشار إلى أن الشرطة تحقق في ضلوع المرأة المحتمل في الجريمة قائلا "علينا أن نثبت أنها اضطلعت بدور (في الجريمة) لكن ذلك قد يكون صعبا".

وعلى الصعيد ذاته أكد مسؤول بمنطقة بنجكولو جنوب غرب سومطرة الأندونيسية إن موقع التواصل الاجتماعي (فيس بوك) أصبح أداة تواصل شعبية جدا في أندونيسيا ، ولكنه يعتقد الآن أن يكون عاملا مساهما في زيادة معدل الطلاق بينجكولو.

وأضاف إن عدد دعاوى الطلاق سجلت ما مجموعه 26 حالة وهو تقريبا ضعف العدد عن نفس الفترة من العام الماضي وإن معظم حالات الطلاق كانت نتيجة قيام أحد الطرفين علاقة افتراضية مع شخص ثالث من خلال الفيس بوك ، وإن معظم الحالات اكتشفت عن طريق المعارف من شبكة الانترنت .

وتشير التقديرات إلى أن معدل الطلاق في عام 2012 مستمر في الارتفاع وفي عام 2011 سجلت المحكمة 448 من حالات الطلاق التي أسفرت عن 245 فقط من الإنهاء الفوري للسند العائلي في يناير 2011 بينما قدمت 12 حالة فقط ، ولكن في عام 2012 كان العدد يقترب من 30 حالة.



وفي تركيا قتل شاب زوجته بسبب إعادة تفعيل صفحتها على موقع التواصل الاجتماعي "فيسبوك"، وأفادت وسائل إعلام تركية أن سيزيز يماز البالغ من العمر 26 عاماً وزوجته بيذا يماز تشاجرا بعنف لدى اكتشافه أنها أعادت تفعيل حسابها على "فيسبوك" مؤخراً، فأطلق النار عليها أمام طفليها "3 أعوام وعام واحد".

واتصل الجيران بالشرطة، فيما قضت المرأة التي كانت قد رفضت الطلاق بسبب طمليها في مكان الحادثة...

وفي محافظة كركوك إحدى محافظات العراق أعلنت وزارة الداخلية، عن تحرير طالبة في كركوك بعد 24 ساعة على اختطافها بعد إغوائها عن طريق الفيسبوك، فيما أشارت إلى اعتقال الخاطفين.

وذكر بيان رسمي إن "قوة من الشرطة تمكنت، من اعتقال أربعة أشخاص متهمين بختطف فتاة في محافظة كركوك"، لافتاً إلى أن "أحد الخاطفين استدرج الفتاة، وهي طالبة، عن طريق الموقع الاجتماعي فيسبوك بحجة الزواج منها والسفر إلى خارج العراق".

وأضاف أن "الشرطة تتبعت الموضوع عبر معلومات استخبارية وتمكنت من تحريرها". يشار إلى أن العلاقات أخذت تتوسع بشكل كبير بين الشبان والشابات في البلاد إثر انطلاق موقع الفيسبوك على الانترنت، الأمر الذي يمزوه مراقبون إلى الحرمان الذي مر به العراق خلال السنين الماضية .

■ لعبة القمار

تنتشر ابدية القمار على الإنترنت وعادة ما تكون محل اشتباه ومراقبة من قبل السلطات الامريكية . وبالرغم من ان سوق القمار في امريكا يعتبر الاسرع نمواً على الاطلاق الا ان المشكلة القانونية التي تواجه اصحاب مواقع القمار الافتراضية على الإنترنت انها غير مصرح لها حتى الان في امريكا بعكس نوادي القمار الحقيقية كالمستشرة في لاس فيجاس وغيرها ، ولذلك يلجأ بعض اصحاب تلك المواقع



الافتراضية على الإنترنت إلى أنشائها وإدارتها من أماكن مجاورة لأمريكا وخاصة في جزيرة أنتيغوا على الكاريبي .

ويوجد على الإنترنت أكثر من ألف موقع للقمار يسمح لمرتاديه من مستخدمي الإنترنت ممارسة جميع أنواع القمار التي توفرها المواقع الحقيقية، ومن المتوقع أن ينفق الأمريكيون ما يزيد عن (600) مليار دولار سنوياً في أندية القمار وسيكون نصيب مواقع الإنترنت منها حوالي مليار دولار.

وقد حاول المشرعون الأمريكيون تحريك مشروع قانون يمنع المقامرة عبر الإنترنت ويسمح بملاحقة الذين يستخدمون المقامرة السلوكية أو الذين يروجون لها سواء كانت هذه المواقع في أمريكا أو خارجها .

■ تجارة المخدرات

لم تقتصر المواقع المنتشرة على الانترنت بالترويج للمخدرات بل تعداه إلى تعليم كيفية زراعة وصناعة المخدرات بكافة أصنافها وأن أنواعها وبأبسط الوسائل المتاحة والأمر الذي يدفع بالقارئ ومعظمهم من المراهقين إلى تطبيق ما يقرأه .
ويلكد هذه المخاوف أحد الخبراء التربويين في بالولايات المتحدة والذي أكد إن ثمة علاقة يمكن ملاحظتها بين ثلوث المراهقة والمخدرات.

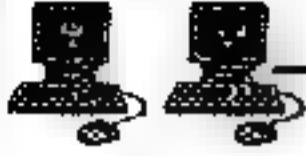
ولا تقتصر ثقافة المخدرات على تلك المواقع فقط بل تساهم المنتديات وغرف الدردشة في ذلك أيضاً .

وبالرغم من انتشار المواقع الخاصة بالترويج للمخدرات وتعليم كيفية صنعها إلا أن هذه المواقع لم تدق جرس الإنذار بعد ولم يهتم بأثارها السلبية وخاصة على النشء كما فعلته المواقع الاباحية وخاصة في الدول التي تعرف باسم الدول المتقدمة

■ جرائم الاتجار بالبشر عن طريق الانترنت

وتتمثل هذه الجريمة بإنشاء أو نشر موقع على شبكة الانترنت بقصد الاتجار بالبشر أو تسهيل التعامل به بأي شكل من الأشكال أو روج له أو ساعد على ذلك أو تعاقد أو تعامل أو تفاوض بقصد إبرام الصفقات المتعلقة بالاتجار بالبشر





ان المخاوف من استخدام الانترنت لا تقتصر على ارتكاب الانترنت في ارتكاب الجريمة بل تساهم بعض المواقع في انحراف الشباب وخصوصا من المراهقين وذلك من خلال انشاء مواقع الالكترونية بقصد الاتجار بالمخدرات و المؤثرات العقلية او الترويج لها او تعاطيها او سهل التعامل فيها او تعاقد او تعامل و تعاوض بقصد ابرام الصفقات المتعلقة بالاتجار بها بأي شكل من الاشكال .

4 - الجرائم الثقافية

تعرف الجرائم الثقافية على انها استيلاء المجرم على الحقوق الفكرية ونسبها له من دون موافقة الضحية فمن الممكن أن تكون احد الصور التالية :

- قرصنة البرمجيات: هي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على اسطوانات وبيعها للناس بسعر أقل .
- "التعدي على القنوات الفضائية المشفرة وإتاحتها عن طريق الانترنت عن طريق تقنية " (soft copy) .
- "جريمة نسخ المؤلفات العلمية و الأدبية بالطرق الالكترونية المستعصنة.

■ جرائم قرصنة البرامج

تعرف قرصنة البرامج بانها الاعتداء بالنسخ أو الاستعمال غير المشروع لبرامج الكمبيوتر المحمية بموجب قوانين حق المؤلف، وطبقا لإحصائية اتحاد منتجي البرامج لعام 2000 تصل نسبة القرصنة إلى 56 ٪ بينما تقدر الخسائر ب12 مليون دولار وتلحق قرصنة البرامج الضرر بكل الشركات المنتجة لبرامج الكمبيوتر بالإضافة إلى المستخدمين أنفسهم، وهي تؤدي إلى ارتفاع أسعار البرامج بالنسبة إلى المستخدمين وإلى انحدار مستوى الدعم الفني للبرامج كما أنها تسبب في تأخر تمويل عمليات تطوير برامج جديدة مما يؤدي بالتالي إلى تدهور مستوى صناعة البرامج ككل.

كذلك تلحق القرصنة أضرارا بكل من ناشري وموزعي برمج الكمبيوتر أيا كان حجمهم، فمطورو البرامج ينفقون أعواما لتطوير برنامج، وهناك جزء من





المقابل المالي الذي يحصل عليه مطورو البرنامج يوجه إلى تطوير برامج جديدة بحيث تستمر تلك البرامج في التطور والتقدم نحو الأفضل.

أما عندما تشتري نسخ البرامج المسروقة، تذهب أموالك مباشرة إلى جيوب قراصنة البرامج.

وتسبب قرصنة البرامج إلى الاقتصاد المحلي، إذ أن انخفاض حجم مبيعات البرامج الأصلية ينتج عنه انخفاض في العائدات وازدياد في البطالة. كما تقف قرصنة البرامج عقبة في وجه تطوير صناعة برامج الكمبيوتر المحلية.

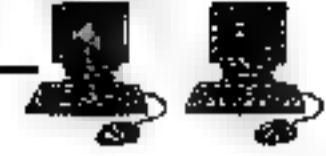
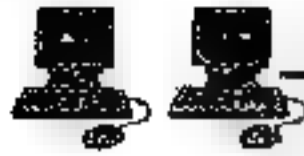
فإذا لم يستطع مطورو البرامج تسويق منتجاتهم تحت حماية القانون، فلن يكون لديهم الحافز للاستمرار في عمل هذه البرامج.

وقد يكون مطورو البرامج المصريين أكبر من يتعرض لمخاطر قرصنة البرامج، فمن شأن الجهد الضخم الذي يتم بذله في مجال الأبحاث والتطوير والاستثمارات والتكلفة العالية التي تتطلبها تطوير البرامج، أن تعرض صفار المطورين من الشركات أو الأفراد لمخاطر اقتصادية من جراء القرصنة.

ومع ذلك فإن المطورين صفار الحجم عادة ما يكونون، معينا أساسيا لأفكار إبداعية في مجال البرامج، وهي أفكار حيوية ليس فقط بالنسبة لكبرى شركات البرامج ولكن أيضا لاستمرار تطور مجتمع تكنولوجيا للمعلومات بأسره. إذا فالمحصلة النهائية للقرصنة هي انخفاض فرص العمل وإعاقة الإبداع في مجال صناعة البرامج في مصر. ولذا لا بد أن تقوم السلطات والمؤسسات والأفراد ببذل الجهد لمكافحة القرصنة وإيجاد قوانين لحماية الملكية.

وكشفت جمعية منتجي برامج الحاسوب التجارية (بي.أس.أي) عن تفاصيل الدراسة العالمية السنوية التاسعة حول قرصنة البرمجيات، حيث ظهر أن المعدل الإجمالي لقرصنة البرمجيات في الشرق الأوسط وأفريقيا بلغ 58٪ عام 2011، في حين وصلت القيمة التجارية للبرمجيات غير المرخصة نحو 4.2 مليارات دولار.





ووجدت الدراسة على الصعيد العالمي أن معدلات القرصنة في الأسواق الناشئة تموق مثيلاتها في الأسواق المستقرة بنسبة 768٪، كما تستحوذ الأسواق الناشئة على الحصة الأكبر من الزيادة العالمية في القيمة التجارية لسرقة البرمجيات. وهذا ما يقصر ديناميكيات السوق وراء المعدل العالمي لقرصنة البرمجيات الذي بلغ نحو 42٪ عام 2011 مع توسع الأسواق في الدول النامية، لتصبح القيمة التجارية للبرمجيات غير المرخصة 63.4 مليار دولار.

وأكدت الجمعية على أهمية اتخاذ السلطات المحلية المزيد من الخطوات المهمة للحد من معدلات القرصنة في دول مجلس التعاون الخليجي.

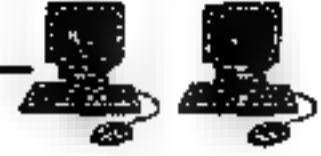
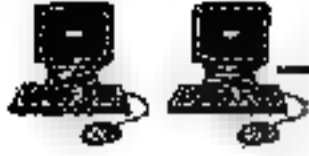
وقال رئيس الجمعية في منطقة الخليج العربي جواد الرضا إن لجمعية ملتزمة بتكثيف مبادرات مكافحة القرصنة في المنطقة للحد من مستوياتها، وهي تعمل عن كثب مع الجهات الحكومية الرئيسية ومؤسسات القطاع الخاص لخلق المزيد من الوعي حول الآثار السلبية لانتهاكات حقوق الملكية الفكرية وقرصنة البرمجيات.

من جهة أخرى كشفت الدراسة أن أكثر قرصنة البرمجيات على الصعيد العالمي هم من الرجال وينتمون بنسب متفاوتة إلى جيل الشباب، وتبلغ احتمالية عيشهم في الاقتصادات الناشئة بمعدل أكثر من الضعف مقارنة بغيرهم في الاقتصادات المستقرة.

كما أظهرت أن صناع القرار في قطاع الأعمال يعترفون بأنهم يستخدمون البرمجيات المقرصنة بصورة أكبر مقارنة بغيرهم من المستخدمين الآخرين. كما يشترون البرنامج لثييته على حاسوب واحد ثم يثبتونه مرة أخرى على أجهزة إضافية في مكاتبهم بمعدل الضعف مقارنة بغيرهم.

ونبهت الدراسة إلى عدم وجود حافز لدى القرصنة لتغيير سلوكهم عمليا، حيث إن 20٪ فقط من القرصنة المألوفين في الأسواق المستقرة و15٪ منهم في الأسواق الناشئة، يعتقدون بأن خطر القبض عليهم سبب لعدم قرصنة البرمجيات.





يذكر أن هذه هي الدراسة السنوية التاسعة حول قرصنة البرمجيات التي تجريها جمعية منتجي برامج الحاسوب التجارية بالتعاون مع مؤسسة أي.دي.سي ومعهد إيبسوس للشؤون العامة اللذين يعتبران من الشركات العالمية المستقلة والرائدة في مجال الأبحاث.

وتتضمن منهجية الدراسة جمع نحو 182 مشاركة منفصلة للبيانات وتقييم اتجاهات الحواسيب والبرمجيات في 116 سوقا. وشملت الدراسة هذا العام 15 ألفا من مستخدمي الحاسوب من 33 دولة، يشكلون معا نحو 82٪ من حجم سوق أجهزة الحاسوب العالمي.

وقد تعرضت حسابات آلاف الأشخاص في خدمة البريد الإلكتروني "هوت ميل" للاختراق في عملية قرصنة كبيرة.

وذكرت شركة مايكروسوفت الأمريكية التي تملك خدمة البريد الإلكتروني أن أكثر من 10 آلاف حساب بريد تم اختراقه وتم نشر كلمات السر لهذه الحسابات على شبكة الانترنت.

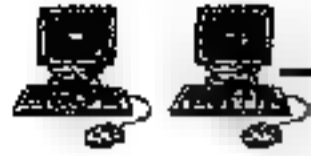
وقالت الشركة إنها أطلقت تحقيقا في الموضوع مبينة أن المعلومات التي تم الحصول عليها بشكل غير قانوني نشرت على شبكة الانترنت.

وأكدت الشركة أنه بمجرد معرفتها طلبت إزالة هذه المعلومات من الشبكة وأطلقت تحقيقا حول مدى تضرر عملاء الشركة.

ويستخدم قراصنة شبكة الانترنت تقنية تسمى "فيشينج" على نحو واسع وهي تنطوي على خداع المستخدمين من أجل انتزاع المعلومات منهم أو من أجل تحميل البرامج المؤذية على حواسيبهم.

ويحد من بين الاستراتيجيات المستخدمة إرسال الرسائل الإلكترونية الزائفة الملحقة بملفات مرفقة تعد يتأمن صور عارية للمشاهير أو إرسال صلات صوب نسخ تبدو مقنعة، لصفحات بلوغ مواقع قانونية.

ونصحت مايكروسوفت مستخدمي الانترنت بالحد من فتح ملفات مرفقة لم يطلبوها أو صلات مجهولة أو غير معروفة المصدر، ونصحتهم أيضا بتجهيز



حواسيبهم ببرامج مكافحة الفيروسات التي يتم تحديثها يوميا ، فضلا عن تغيير كلمة السر كل 90 يوما تقريبا.

يشار إلى أن قرصنة البريد الإلكتروني لا تقتصر فقط على اختراقه ، بل من خلال المزيد من الرسائل غير المرغوبة التي تنهال على مستخدمي الانترنت يوميا ، حيث أصبحت إحدى الشركات المعنية بالأمن الإلكتروني أن هناك زيادة في نشاط مجرمي الانترنت في العمل.

وكشفت الشركة أن حجم رسائل البريد الإلكتروني من نوع "سبام" التي يتم إرسالها يوميا ، وصل إلى حوالي 180 مليار رسالة ، أي حوالي 90 / من إجمالي حجم البريد الإلكتروني المرسل في كافة أرجاء العالم.

وكان تقرير سابق عن الأمن الإلكتروني لشركة مايكروسوفت الأمريكية قد كشف أن 97 / من البريد الإلكتروني رسائل غير مرغوب فيها ، مشيرا إلى أن معظم البريد الإلكتروني عبارة عن إعلانات متطفلة عن عقاقير، ومنتجات خردة وغالبا ما تكون مصحوبة بملفات ضارة.

وأوضح إد جيبسون كبير مستشاري الأمن الإلكتروني بمايكروسوفت ، قوله إن ارتفاع معدلات البريد الإلكتروني غير المرغوب فيه يمس تحول الجريمة المنظمة عن استغلال ثغرات البرامج الإلكترونية واستهدافها مستخدمي الشبكة العاديين ، بفعل تطور خدمات الانترنت وسرعة تدفقها.

■ انتهاك الخصوصية:

تتفق التشريعات السماوية والأنظمة الوضعية على ضرورة احترام خصوصية الفرد ويعتبر مجرد التطفل على تلك المعلومات سواء كانت مخزنة في الحاسب الآلي أو في بريدك الإلكتروني أو في أي مكان آخر انتهاكاً لخصوصيته الفردية.

وأدى انتشار الإنترنت إلى تعرض الكثير من مستخدمي الإنترنت لانتهاك خصوصياتهم الفردية سواء عمدا أو مصادفة ، فبكل بساطة ما أن يزور مستخدم الإنترنت أي موقع على شبكة الإنترنت حتى يقوم ذلك الموقع بإصدار نسختين من الكعكة الخاصة بأجهزتهم (Cookies) وهي نصوص صغيرة يرسلها العديد من





مواقع الويب لتخزينها في جهاز من يزور تلك المواقع لعدة اسباب لعل منها التعرف على من يكرر الزيارة للموقع أو لأسباب أخرى، وتبقى واحدة من الكعكات في الخادم (السيرفر) الخاص بهم والأخرى يتم تخزينها على القرص الصلب لجهاز الزائر للموقع في أحد الملفات التي قامت الموقع الأخرى بتخزينها من قبل دون أن يشعر صاحب الجهاز بذلك أو حتى الاستئذان منها وفورا يتم اصدار رقم خاص ليميز ذلك الزائر عن غيره من الزوار وتبدأ الكعكة بأداء مهمتها بجمع المعلومات وإرسالها إلى مصدرها أو إحدى شركات الجمع والتحليل للمعلومات وهي عادة ما تكون شركات دعاية وإعلان وكلما قام ذلك الشخص بزيارة الموقع يتم إرسال المعلومات وتجديد النسخة الموحدة لديهم ويقوم المتصفح لديه بعمل المهمة المطلوبة منه ما لم يقوم صاحب الجهاز بتعديل وضعها، وقد تستغل بعض المواقع المشبوهة هذه الكعكات بنسخ تلك الملفات والاستفادة منها بطريقة أو بأخرى.

كما قد يحصل اصحاب المواقع على معلومات شخصية لصاحب الجهاز طوعا حيث يكون الشخص عادة أقل ترددا عندما يفشى معلوماته الشخصية من خلال تعامله مع جهاز الحاسب الآلي بعكس لو كان الذي يتعامل معه انسان اخر. وهناك وسائل لحماية الخصوصية اثناء تصفح الإنترنت ، ولكن " من الصعب جدا السيطرة على ما يحدث للمعلومة بمجرد خروجها من جهاز الحاسب (الآلي) وعلى ذلك فان حماية الخصوصية يجب ان تبدأ من البداية بتحديد نوعية البيانات التي لا ينبغي ان تصبح عامة ومشاعة ثم بتقييد الوصول إلى تلك المعلومات " .

5 - الجرائم السياسية

تتعدد أشكال الجريمة السياسية ومنها :-

- تستخدم المجموعات المسلحة حالياً تقنية المعلومات لتسهيل الأشكال المغطية من الأعمال الإجرامية. وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل، الاتصالات والتمسيق، وبث الأخبار المغلوطة، وتوظيف بعض صغار السن، وتحويل بعض الأموال في سبيل تحقيق أهدافهم.





- الاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر الفيروسات وذلك يرجع إلى العدد المتزايد من برامج الكمبيوتر القوية والسهلة الاستخدام والتي يمكن تحميلها مجاناً .
- نشر الأفكار الخاطئة بين الشباب كالإرهاب والإدمان والزنا لفساد الدولة لأسباب سياسية واقتصادية بالدرجة الأولى .

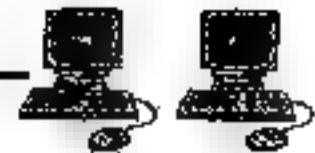
■ المواقع المعادية :

يسكثر انتشار الكثير من المواقع الغير المرغوب فيها علي شبكة الإنترنت فمصطلح المواقع المعادية هو مصطلح حديث بدأ استخدامه بعد هذا التطور التكنولوجي في مجال شبكة الإنترنت فقام مصممي المواقع المعادية باستغلال التكنولوجيا لخدمة أغراضهم الشخصية : ومن هذه المواقع ما يكون موجهاً ضد سياسة دولة ما أو ضد عقيدة أو مذهب معين أو حتى ضد شخص ما . وهي تهدف في المقام الأول الى تشويه صورة الدولة أو المعتقد أو الشخص المستهدف . وتصنف المواقع المعادية وفقاً للفرض منها كالآتي :-

1- المواقع السياسية المعادية:

قد ينظر البعض إلى إنشاء تلك المواقع كظاهرة حضارية تتمشي مع الديمقراطية والحرية الشخصية ، ولكن الواقع غالباً ما يكون الفرض من وراء إنشائها هي معارضة النظام السياسي القائم في بلد ما فيحاولون من خلال تلك المواقع نشر الأخبار الفاسدة التي تشر الفارقة بين أفراد الشعب ونظامه السياسي القائم .

فقد صدق مكتب التصديق على الاحكام بمجلس الوزراء على الحكم الي اصدارته محكمة امن الدولة العليا ضد جميع المتهمين في قضية حزب التحرير والبالغ عددهم 26 متهما ، وعاقبت المحكمة 12 متهما بينهم ثلاثة بريطانيين بالسجن 5 سنوات ، 7 متهمين بالسجن 3 سنوات ، وستة واحدة لـ 7 متهمين آخرين حيث انه في عام 2002م اتهمت نيابة امن الدولة العليا المذكورين بالترويج بالقول والكتابة لاغراض جماعة اسمت على خلاف احكام القانون تسمى حزب التحرير ،



وتدعو الى تعطيل احكام الدستور والقانون ، ومنع مؤسسات الدولة من مباشرة عملها والترويج لافكار الحزب غير المنشورات، وانشاء موقع على شبكة الإنترنت يدعو لهذه الافكار ، وتكفير النظم الحاكمة.

2- المواقع الدينية المعادية :

ويكون الغرض من وراء إنشائها الإساءة إلى دين معين من الأديان ونشر الأفكار السيئة عنه وحث الناس على الابتعاد عنه ، وتلك المواقع غالباً يكون القائمين عليها من معتقي الديانات الأخرى المتشددون في دينهم ، أو أن يكون هدفهم بث الشقاق والخلاف في ما بين أفراد الشعب الواحد فيحاولون إثارة الفتنة عن طريق نشر الأخبار الكاذبة والمندسوسة وذلك لتحقيق هدفهم الخبيث .

3- المواقع المعادية للأشخاص أو الجهات :-

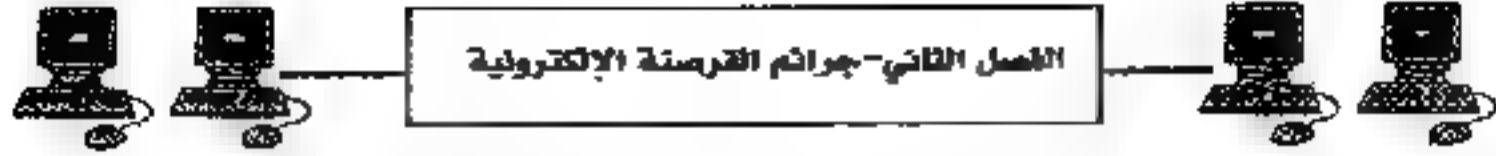
وهي تشبه إلى حد كبير بالمواقع المخصصة للقذف ، حيث تهدف أساساً لتشويه سمعة الشخص أو الجهة .

انتحال الشخصية وينقسم الى نوعين :-

أ - إنتحال شخصية الفرد:

تعتبر جرائم انتحال الشخصية من الجرائم القديمة الا ان التنامي المتزايد لشبكة الإنترنت اعطى المجرمين قدرة اكبر على جمع المعلومات الشخصية المطلوبة عن الضحية والاستفادة منها في ارتكاب جرائمهم. فتنتشر في شبكة الإنترنت الكثير من الاعلانات المشبوهة والتي حاول البعض الاستيلاء على معلومات اختيارية من الضحية، فهناك مثلاً اعلان عن جائزة فخمة يكسبها من يساهم بمبلغ رمزي لجهة خيرية والذي يتطلب بطبيعة الحال الافصاح عن بعض المعلومات الشخصية كالاسم والعنوان والأهم رقم بطاقة الائتمان لخصم المبلغ الرمزي لصالح الجهة الخيرية ، وبالرغم من ان مثل هذا الاعلان من الواضح يمكن انه عملية نصب واحتيال الا انه ليس من المستبعد ان يقع ضحيته الكثير من مستخدمي الإنترنت . ويمكن ان تؤدي جريمة انتحال الشخصية إلى الاستيلاء على رصيده البنكي أو السحب من بطاقته الائتمانية أو حتى الاساءة إلى سمعة الضحية.





ب - انتحال شخصية المواقع :

مع ان هذا الاسلوب يعتبر حديث نسبيا الا انه اشد خطورة واكثر صعوبة في اكتشافه من انتحال شخصية الافراد ، حيث يمكن تنفيذ هذا الاسلوب حتى مع المواقع التي يتم الاتصال بها من خلال نظم الاتصال الامن (Secured Server) حيث يمكن وبسهولة اختراق مثل هذا الحاجز الامني ، وتتم عملية الانتحال بهجوم يشنه المجرم على الموقع للسيطرة عليه ومن ثم يقوم بتحويله كموقع بديلي ، أو يحاول المجرم اختراق موقع ل احد مقدمي الخدمة المشهورين ثم يقوم بتركيب البرنامج الخاص به هناك مما يؤدي إلى توجيه أي شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور.

ويتوقع ان يكثر استخدام اسلوب انتحال شخصية المواقع في المستقبل نظرا لصعوبة اكتشافها.

■ استخدام الانترنت في ارتكاب الجريمة المنظمة :-

وهي استخدام شبكة الانترنت بقصد اشاعة الفوضى بقصد اضعاف النظام او الثقة بالنظام الالكتروني للدولة او اتلاف وتعطيل او اعاقه او الاضرار بأنظمة الحاسوب او شبكة المعلومات العائدة للدولة بقصد المساس بنظامها ، او البنى التحتية ونشر او اذاعة وقائع كاذبة او مظلة بقصد اضعاف الثقة بالنظام المالي الالكتروني او الاوراق التجارية والمالية الالكترونية وماقي حكمها بقصد الاضرار بالاقتصاد الوطني والثقة المالية للدولة واستخدام الانترنت في ارتكاب جرائم غسيل الاموال حيث يأخذ المجرمون باحدث التقنيات لغرض خدمة نشاطاتهم سيما وان جرائم غسيل الاموال عابرة للحدود.

تزوير البيانات من الجرائم المعلوماتية الاكثر انتشارا فلا تكاد تخلو جريمة من جرائم نظم المعلومات من شكل من اشكال التزوير للبيانات من خلال تزوير او تقليد او اصطناع توقيع او سند او كتابة الكترونية او اية وسيلة اخرى او استعمال البطاقة الالكترونية المقلدة او المزورة مع علمه بذلك او اصطناع عمدا وثائق



أو سجلات أو قيود الكترونية أو أحدث تغيير أو تلاعب في سند الكتروني صحيح و الاستيلاء عمداً على توقيع أو كتابة أو سند واستخدامها لمصلحة الشخصية .

6 - الجرائم الجنسية

هذا النوع من الجريمة يمكن أن يتخذ إحدى الصور التالية :

أ - الابتزاز : من أشهر حوادث الابتزاز عندما يقوم أحد الشباب باختراق جهاز أحد الفتيات أو الاستيلاء عليه و به مجموعة من صورها ، وإجبارها على الخروج معه وإلا سيفضحها بما يملكه من صور .

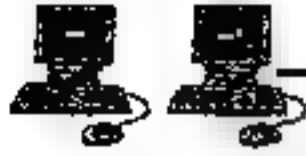
ويأتي الابتزاز من خلال تهديد الجاني ضحيته بنشر صور خاصة جداً لها في موقع الإنترنت المختلفة ، وعبر البلوتوث أو أجهزة البلاك بيري أو البرامج المختلفة المرفقة بأجهزة الهواتف الذكية مثل برنامج الواتس آب؛ إن لم ترضخ له وتستجيب لمطالبه سواء كانت تلك المطالب مادية أو معنوية.

ومنه قيام أحد المخربين بسرقة بيانات البريد الرقمي لإحدى الفتيات ومساومتها على تزويده بمبالغ مالية وفي حال رفضت ذلك سيقوم بنشر صورها في مواقع الإنترنت بعد أن يقوم بعمل دبلجة للوحة مع أجساد عارية من خلال برنامج الفوتوشوب، وفي حال استجابتها لطلبه فسوف يعيد لها كلمة المرور الخاصة بعنوانها البريدي .

ب - التفرير والاستدراج : في العادة تتواجد هذه الصورة عندما يتعرف أحد الشبان على إحدى الفتيات في الشات أو في برامج المحادثة ويكوّن علاقة معها ثم يستدرجها بالكلام المعسول ويوهمها بالزواج لكي تثق به ومن ثم يقوم بتهديدها وفصيحته بما يملكه من صور أو تسجيلات لصوتها إن لم تستجيب لطلباته .

ج - انتشار الصور و مقاطع الفيديو المخلة بالأداب على مواقع الانترنت من قبل الفرو الفكرى لكي يتدوالها الشبان والشابات وإفساد أفكارهم وإضعاف إيمانهم .





7 - الجريمة المادية (Financial Crime) :

وهي التي تسبب أضراراً مالية على الضحية أو المستهدف من عملية النصب وتأخذ واحدة من الأشكال الثلاثة التي سوف أستعرضها بشرح مختصر مثل:

- عملية السرقة الإلكترونية كالاستيلاء على ماكينات الصرف الآلي والبنوك كتلك المنتشرة الآن في الكثير من الدول الأفريقية وخاصة جنوب إفريقيا وفيها يتم نسخ البيانات الإلكترونية لبطاقة الصراف الآلي ومن ثم استخدامها لصرف أموال من حساب الضحية .

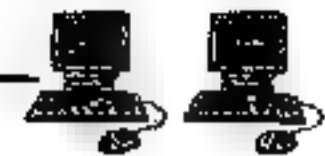
- إنشاء صفحة انترنت مماثلة جداً لموقع أحد البنوك الكبرى أو المؤسسات المالية الضخمة (phishing) لتطلب من العميل إدخال بياناته أو تحديث معلوماته بقصد الحصول على بياناته المصرفية وسرقتها .

- "رسائل البريد الواردة من مصادر مجهولة بخصوص طلب المساهمة في تحرير الأموال من الخارج مع الوعد بنسبة من المبلغ، أو تلك التي توهم صاحب البريد الإلكتروني بفوزه بإحدى الجوائز أو اليانصيب وتطالبه بموافاة الجهة برقم حسابه المصرفي" .

■ الاغراق بالرسائل

يلجأ بعض الأشخاص إلى ارسال مئات الرسائل إلى البريد الإلكتروني لشخص ما بقصد الاضرار به حيث يؤدي ذلك إلى تعطل الشبكة وعدم امكانية استقبال أي رسائل فضلاً عن امكانية انقطاع الخدمة

وإذا ما تعرض الشخص العادي لمحاولة الاغراق بالرسائل حيث لن يصمد بريد طويل امام هذا العيل المتهمر من الرسائل عديدة الفائدة أو التي قد يصاحبها فيروسات أو صور أو ملفات كبيرة الحجم، خاصة اذا علمنا ان مزود الخدمة عادة يعطي مساحة محددة للبريد لا تتجاوز عشرة ميغا كحد اعلى .



مكافحة جرائم الانترنت

يتم مكافحة جرائم الانترنت من خلال :-

- تنمية دور الأسرة والمجتمع في مواجهة الجريمة الإلكترونية وذلك من خلال النشرات التوعوية وعقد مؤتمرات واث ورق عمل إرشادية على صفحات الإنترنت كذلك إقامة حملات إعلانية لتحذير المراهقات من الارتباط بعلاقات مع مجهولين عبر الإنترنت.
 - مواكبة التقنية الحديثة وتأمينها فور انتشارها وتسخيرها للعمل في مجال الوقاية من الجريمة ومكافحتها مثال على ذلك تشديد الرقابة على أكثر البرامج المتداولة بين الشباب كـ facebook ونشر إرشادات بصفة مستمرة عليه ودعوة مزودي خدمة الانترنت إلى اتخاذ الإجراءات اللازمة لوضع فلتر لحماية الأطفال وتوعية مستخدمي الإنترنت لمخاطر الانترنت وحجب المواقع الإباحية.
 - توفير القوى البشرية المؤهلة والمدربة للعمل على هذه الأجهزة الحديثة وتحقيق أداء عالٍ من خلالها وذلك بالتدريب على تحديد مخاطر حقيقة في الشبكة العنكبوتية. وكيفية مواجهتها (مواجهة الهاكرز) كذلك تصميم الكثير من البرامج التي تعمل على حائط صد هجمات تلك القراصنة ولعل أشهر البرنامج McAfee كذلك التطبيق العملي على الوقاية من مخاطر معينة.
 - أنشئت عام 2006 منظمة تدعى (مجموعة العمل للتحالف الإستراتيجي للجريمة الإلكترونية) مهمتها وضع قوانين للحد من الجريمة الإلكترونية في العالم وذلك بمساعدة منظمات حكومية عالمية .
- وللحيلولة دون وقوع العديد من جرائم الانترنت . هرعت العديد من الشركات الإلكترونية في إنتاج برمجيات الحماية الإلكترونية وهو ما ابتكرته شركة "ماكاي" المتخصصة في إنتاج برمجيات الحماية الإلكترونية من طريقة جديدة لمساعدة مستخدمي الحاسبات الإلكترونية على التعرف على أساليب الاحتيال التي يستخدمها مجرمو الإنترنت.



وتعتمد الطريقة الجديدة من الشركة على طريقة السؤال والجواب فقد طرحت ماكاي على موقعها على شبكة الإنترنت اختباراً يتكون من عشرة أسئلة يخضع إليها الزائرون ليحددوا بأنفسهم إذا كان بإمكانهم إعاقة محاولات سرقة معلومات شخصية عنهم مثل كلمات المرور، وأرقام البطاقات الائتمانية، وذلك أثناء تصفحهم المواقع الإلكترونية ذات الشعبية الواسعة، والتي تضم مواقع التسوق، والشبكات الاجتماعية.

ويتضمن الاختبار ثمانية أسئلة تقدم من خلالهم الشركة نماذج لمواقع إلكترونية ورسائل إلكترونية، ويستعين على المتصفح تحديد بدوره ما إذا كانت حقيقية أم مزيفة، فيما يدور السؤالان الباقيان حول بعض المعلومات العامة حول أساليب الاحتيال عبر الإنترنت.

على جانب آخر، طور قراصنة الانترنت تقنياتهم لتدمير المواقع الإلكترونية وإمكانية استخدام المواقع لتنفيذ برامج تدميرية عدائية على أجهزة الزائرين لهذه المواقع، فبدلاً من إرسال هذه البرامج عبر البريد الإلكتروني والتي تتطلب أن يقوم المستخدم بتنزيل هذه البرامج على جهازه وتنفيذها فإن البريد ربما يحمل وصلة إلى موقع فقط وبمجرد ضغط المستخدم على هذه الوصلة تنتقل إلى الموقع الذي يقوم بباقي المهمة في عملية القرصنة.

وفي محاولة أخرى للحد من جرائم الاحتيال عبر الإنترنت استحدث "الاتحاد الدولي للاتصالات" دليلاً إلكترونياً لتتبع الممارير الأمنية الخاصة بتكنولوجيا المعلومات والاتصالات لمكافحة الجريمة على الإنترنت، ويعتمد على مفهوم أن تنهض جهة مضرّة بذلك التتبع، ما يمكن المعنيين من الرجوع إليها ومتابعتها بسهولة.

ووفقاً للبيان الصحفي للاتحاد الدولي للاتصالات فقد تم وضع دليل بالتعاون المشترك بين "الاتحاد الدولي للاتصالات" و "الوكالة الأوروبية المختصة بأمن الشبكات والمعلومات" وأطراف دولية أخرى مهتمة بشؤون الأمن المعلوماتي على شبكة الانترنت.



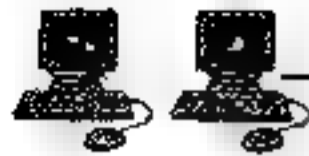


ويعرض الدليل أسماء المنظمات المعنية بتطوير المعايير وما تنشره من صيغ خاصة بأمن الإنترنت، ما يُجَنَّب تكرار الجهود، كما يسهل مهمة مهندسي أمن الشبكة الإلكترونية في كشف الثغرات التي تُمكن العابثين من تهديد أمنها ويضم الدليل خمسة أقسام تُحدَّثُ بصفة مستمرة و تتناول منظمات تطوير المعايير الخاصة بتكنولوجيا المعلومات والاتصالات وأعمالها والصيغ المعتمدة لتلك المعايير وطرق إقرار الاتفاق على تلك المعايير، والحاجات المستقبلية. الشرطة هي خدمة الإنترنت وهي نفس السياق وللمعد من الخطر القادم عبر الشبكات، تسارع الدول إلى وضع ضوابط وحماية وإنشاء أمن خاص للشبكات حيث شكلت وزارة الداخلية المصرية "دوريات أمنية" من خلال الشبكة ، ومهامها منع الجريمة قبل وقوعها.

واستطاعت هذه الدوريات من ضبط تنظيم للشواذ يمارس جرائمه عبر الإنترنت، وكذلك ضبط العديد ممن يحاول استخدام بطاقات ائتمان مسروقة. الحكومة البريطانية أيضاً شكلت وحدة من قوات الشرطة وكلفت بمتابعة المجرمين الذين يستخدمون أجهزة الكمبيوتر وبعد اقتناع تام بالخطر القادم ومداولات استمرت أربع سنوات قامت ثلاثون دولة أوروبية بتوقيع معاهدة لتوحيد الجهود في محاربة جرائم الإنترنت. ومطلوب من أجهزة الأمن العربية أن تواجه هذا التحدي وتطور قدراتها وتحديث برامجها للقضاء أو للحد من مثل هذه الجرائم.

وفي السعودية، تفرض الحكومة عقوبات بالسجن لمدة عام واحد وغرامات لا تزيد عن 500 ألف ريال فيما يعادل 133 ألف دولار لجرائم القرصنة المرتبطة بالإنترنت وإساءة استخدام كاميرات الهواتف المحمولة مثل التقاط صور دون تصريح. وأكد بيان صادر عن الحكومة السعودية موافقتها على مشروع قانون بخصوص جرائم تكنولوجيا المعلومات كان مجلس الشورى السعودي قد اقترحه العام الماضي وبموجب مشروع القانون ، توقع العقوبة على الدخول غير المشروع إلى موقع الكتروني أو الدخول إلى موقع الكتروني لتغيير تصميم هذا الموقع أو إلغائه أو إتلافه أو تعديله ، كما يجرم مشروع القانون "المساس بالحياة الخاصة عن طريق





الفصل الثاني - جرائم القرصنة الإلكترونية



إساءة استخدام الهواتف المحمولة المزودة بكاميرا أو ما في حكمها بقصد التشهير
بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة“



هوامش الفصل الثاني:

- 1 - منتديات نياية ابن امسيك ,
<http://benmsik.ahlamontada.com/t118-topic>
- 2 - موقع ارايبيا، 10/6/2001م .
- 3 - المركز المصري لحماية الملكية الفكرية ، على الموقع التالي:
http://www.ecipit.org.eg/Arabic/homepage_A.aspx,1/1/2009,p.1
- 4 - <http://www.alriyadh.com/2012/08/21/article761709.html>.
- 5 - جريدة الرياض . النسخة الالكترونية من صحيفة الرياض الصادرة عن مؤسسة اليمامة الصحفية الثلاثاء 3 شوال 1433 هـ اغسطس 2012 العدد 161 29
- 6 - جريدة المشرق 04/03/2012
- 7 - " الجرائم الإلكترونية.. الخطر الداهم على المجتمع والأسرة " على الرابط
"<http://www.zoomkw.com/zoom/Article.cfm?ArticleID=76148>" :
أخر زيارة 13- مايو- 2010
- 8 - الجرائم الإلكترونية وأنواعها والأنظمة المطبقة في السعودية " على الرابط :
<http://coeia.edu.sa/index.php/ar/asuurance-awareness/articles/51-forensic-and-computer-crimes/987-types-of-electronic-crime-and-regulations-in-force-in-saudi-arabia.html> " آخر زيارة :
10- مايو - 2010
- 9 - المعجل نبيل الإرهاب والانتترنت " على الرابط:
www.alarabiya.net/views/2005/01/05/9306.html " آخر زيارة :
13- مايو - 2010 .





10 El-Guindy, Mohamed "East Cybercrime in the Middle" على

الرابط: [http://www.ask-pc.com/lessons/CYBERCRIME-](http://www.ask-pc.com/lessons/CYBERCRIME-MIDDLE-EAST.pdf)

MIDDLE-EAST.pdf

11- الرابط: http://fergdawg.blogspot.com/2008_03_16_archive.html

أختر زيارة: 13- مايو 2010.

12- "عمليات الاحتيال المالي تكلف منطقة الخليج 380 مليون دولار" في جريدة

الرياض على الرابط: <http://www.alriyadh.com/2009/01/31/article406176.html>

أختر زيارة 8- مايو- 2010.

13- "خسائرها بالمليارات .. جريمة الكترونية كل 3 دقائق على الانترنت" على

الرابط: [http://www.ensan.net/news/212/ARTICLE/3596/2008-](http://www.ensan.net/news/212/ARTICLE/3596/2008-04-22.html)

04-22.html أختر زيارة: 6- مايو - 2010.

14- العنزي، خالد. "الابتزاز" بصحيفة الإخبارية على الرابط: "

<http://www.klbi.com/articles.php?action=show> id=229&" آخر

زيارة: 8- مايو- 2010.

15 - الجزيرة نت، الأربعاء 1433/6/24 هـ - الموافق 2012/5/16 م

انظر - : [http://www.aljazeera.net/news/pages/73658c46-12b4-](http://www.aljazeera.net/news/pages/73658c46-12b4-4ae5-97c4-27542cf598cf)

4ae5-97c4-27542cf598cf

16 - منتديات العاصفة، 7-10-2009، انظر: -

<http://www.3asfh.net/vb/t113052.html>

17 - جريدة الرياض، جرائم الانترنت تعددت صورها وأشكالها فلم تعد تقتصر

على فتحام الشبكات وتخريبها أو سرقة معلومات منها - تقرير: أسماء أحمد

انظر: - www.alriyadh.com





18 - شبكة النباء المعلوماتية - الأربعاء 17/11/2011 -

16/رمضان/1432.

19 - الحرية الإلكترونية مصطفى سمارة - مجلة المعلوماتية العدد 29 - شهر تموز 2008 .

30 جمهورية العراق . السلطة القضائية مجلس القضاء الاعلى . -10-2012

15 . <http://www.iraqja.iq/view.1645> .

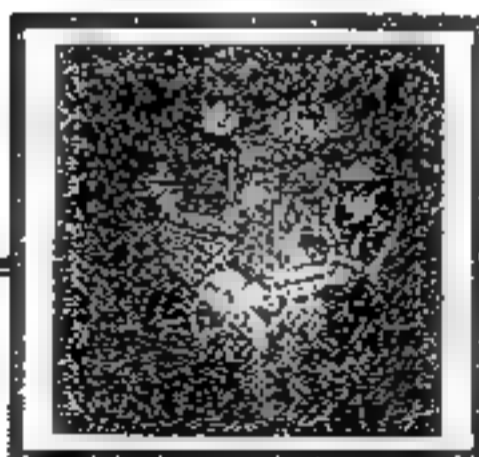


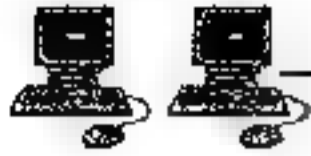


الفصل الثالث

حروب القرصنة

الإلكترونية





مع التطور التكنولوجي غير المسبوق، تراجعت أولوية الحروب المباشرة التي تتخذ من العتاد المادي والبشري وقوداً لها

في حين انتشر ما يسمى بـ"الحرب الإلكترونية" كنمط جديد وأكثر فاعلية للحرب بين دول العالم. حتى أنها صارت وسيلة هامة للغاية في تحقيق الأرباح وتكبّد خسائر فادحة في الوقت نفسه.

إنها حرب تبتعد عن النمط التقليدي للحرب إلى النمط غير التقليدي، وذلك باستخدام تقنيات حديثة كالمطائرات بدون طيار، واستخدام التقنية لاستهداف البنية المعلوماتية للعدو التي تعد القاعدة الأساسية لسير معظم العمليات التكتيكية، بداية من التخطيط ونهاية إلى العمل بها.

وقد أثبتت الدراسات والأبحاث أن حوالي الـ100 هجوم إلكتروني في الثانية، يصيب أماكن ومواقع كثيرة غير محددة من العالم. إلا أن بعض الشركات ذات الأسماء الكبيرة والبنوك، يمتنعون عن التبليغ كي لا يخسروا عملاءهم. الشيء الذي سيحدث بالتأكيد إذا ما شعر العميل أو الزبون بضعف نظام حماية البنك الذي يتعامل معه كمثال.

الحرب الإلكترونية

إن تعبير "الحرب الإلكترونية" يستخدم على نطاق واسع في العالم العربي كمترادف لمصطلح (Cyber War) ويرى باحثون أن هذا التعبير يتداخل مع العديد من المصطلحات ومفاهيم أخرى كالـ (Electronic War) أو (Information War) وهي المستوى الأخطر للنزاع في الفضاء الإلكتروني، وتعتبر جزءاً من الحرب المعلوماتية بمعناها الأوسع، وتهدف إلى التأثير على إرادة الطرف المستهدف السياسية وعلى قدرته في عملية صنع القرار، وكذلك التأثير فيما يتعلق بالقيادة العسكرية و/أو توجهات المدنيين في مسرح العمليات الإلكترونية للحرب الإلكترونية العديد من التعريفات العلمية، إلا أنها بالدرجة الأولى تتوقف على طبيعة الاستخدام القتالي





ومفهومه المطلوب تحقيقهما في العمليات الحربية الحديثة التي تتنوع فيها النظم والوسائل لإلكترونية المتطورة لأسلحة القتال؛ تلك الأهداف المطلوب من الحرب الإلكترونية أن تتعامل معها، وتؤثر على فاعليتها، بهدف حرمانها من أداء مهامها الوظيفية بكفاءة، وبالتالي تهيئة الظروف المناسبة للقوات الصديقة من العمل في بيئة إلكترونية مناسبة تسمح بتنفيذ المهام المطلوبة بكفاءة ودقة عاليتين، وفي الرمان والمكان المناسبين.

فالحرب الإلكترونية إذن هي مجموعة الإجراءات الإلكترونية المتضمنة استخدام بعض النظم والوسائل الإلكترونية الصديقة في استطلاع الإشعاع الكهرومغناطيسي الصادر من نظم، العدو ووسائله ومعداته الإلكترونية المختلفة مع الاستخدام المتعمد للطاقة الكهرومغناطيسية في التأثير على هذه النظم والوسائل؛ لمنع العدو، أو حرمانه، أو تقليل استغلاله للمجال الكهرومغناطيسي، فضلاً عن حماية الموجات الكهرومغناطيسية الصادرة من النظم والوسائل الإلكترونية الصديقة من استطلاع العدو لها، أو التأثير عليها.

ولذلك يحدّد استخدام تعبير "حرب الإنترنت والشبكات" على الرغم من أنه قد لا يفي بالفرض إلا أنه يعد أكثر تحديداً في تعريف الـ (Cyber War).

وتشير العديد من التقارير إلى تزايد أعداد الهجمات الإلكترونية التي تتم في العالم اليوم والتي تقوم بها مجموعات أو حكومات تتدرج في الاستهداف من أبسط المستويات إلى أكثرها تعقيداً وخطورة.

وعرف كل من "ريتشارد كلارك" و"روبرت كناكي" الحرب الإلكترونية على أنها "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها".

فيما يعرف آخرون مصطلح الحرب الإلكترونية بأنها "مفهوم يشير إلى أي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي".

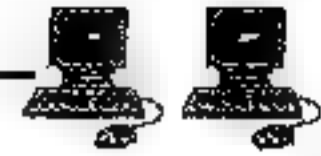
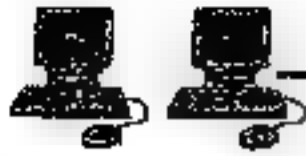
وتختلف الحرب الإلكترونية عن الحروب العادية بعدة أمور منها:

1 - محال الحرب الإلكترونية أوسع من أن يتولاها بضعة أشخاص .



- 2 - والقطاعات المستهدفة أكبر .
 - 3 - والأضرار الناجمة أضخم .
 - 4 - والقدرات المستخدمة هائلة.
 - 5 - والحرب الإلكترونية لا تحتاج إلا لدول لديها القدرة والقابلية على استثمار مواردها في هذا الإطار واستخدامها في هذا المجال.
- وبناء عليه تعاملت دول العالم كافة مع الحرب الإلكترونية إلا أنها تتفاوت في قدراتها وبناء جيوش من الخبراء الذين قد يشكلون مستقبلا نواة الجيش الإلكتروني للدولة . لذا يمكن توزيع تلك الدول الى مراتب كالآتي:
- المرتبة الأولى؛ وتشمل الصين وروسيا والولايات المتحدة الأمريكية وفرنسا وباكستان وإسرائيل .
- المرتبة الثانية؛ وتشمل الهند وباكستان .
- المرتبة الثالثة؛ وتشمل كوريا الشمالية وإيران .
- فيما يعمل عدد آخر من الدول بصمت ومنها :-
- 1 - الألمان فهم يتمتعون بقدرات عالية ومتطورة، ولكنها مقيّدة ويتم كبحها بدافع ذاتي خاصة في الأعمال السرية.
 - 2 - أمّا الروس والصينيون، فهم ليسوا كذلك على الإطلاق وهناك نزعة هجومية واضحة في عملهم، وتنسب إليهم معظم الهجمات التي تتم اليوم في الفضاء الإلكتروني من خلال تنظيمهم آلاف الهجمات على مواقع أجنبية كل عام.
- فقد كانت الشكوك تحوم حول الروس في أشهر حالتين معروفتين في هجمات أستونيا ربيع عام 2007 وجورجيا صيف عام 2008.
- 3 - أمّا الصينيون فقد شنوا العديد من الهجمات الشرسة المعروفة حتى اليوم في مجال التجسس لعل أهمها محاولات اختراق البنّاغون في العام 2007.





تاريخ الحرب الإلكترونية العالمية

عند تتبع تاريخ نشأة الحرب الإلكترونية في العالم، نجد أن جذورها تعود لما قبل اندلاع الحرب العالمية الأولى، فقد بدأت الاتصالات بين أرجاء العالم المختلفة باستخدام المواصلات السلكية من طريق المورس "جهاز البرق الصوتي" عام 1837؛ ولم يتحقق أي اتصال آخر في ذلك الوقت إلا من طريق تبادل المراسلات؛ باستخدام السفن في نقل الرسائل بين الموانئ البحرية.

منذ اندلاع الحرب الأهلية في الولايات المتحدة الأمريكية، في أبريل 1861، كانت خطوط التلفراف هدفاً مهماً للقوات المتعاربة؛ إذ كان عمال الإشارة يتدخلون على خطوط المواصلات السلكية، من طريق توصيل هاتف على التوازي مع كل خط من هذه الخطوط؛ للتصت على المحادثات؛ ولهذا السبب، كان كل جانب يقطع المواصلات الخطية عند عدم الحاجة إليها، حتى لا يتداخل عليها الطرف الآخر.

ثم كانت بداية استخدام الاتصال اللاسلكي في عام 1888 مع الألماني هرتز Hertz. وفي منتصف عام 1897 استطاع "ماركوني" Guglielmo Marconi المهندس والمخترع الإيطالي من تطوير جهاز لاسلكي يناسب الاستخدام في البحر. ثم استخدم اللاسلكي في أعمال الاتصالات بالمرسح البحري الأوروبي في عام 1901.

ونتيجة لتزايد الاستخدام اللاسلكي، كان طبيعياً أن تظهر الشوشرة على الاتصالات اللاسلكية، وكانت في البداية شوشرة طبيعية، نتيجة لكثرة استخدام الأجهزة اللاسلكية، وهو ما يعرف بالتداخل البيئي للموجات الكهرومغناطيسية عند إشعاعها بكثافة عالية في مساحة محددة، أو في مناطق مغلقة، مثل المضائق والممرات الجبلية.

ومن هنا بدأ التدريب على العمل في ظل الشوشرة نتيجة الاستخدام اللاسلكي المكثف، ثم بدأ الاستخدام المتعمد للشوشرة؛ لإعاقة الاتصالات





اللاسلكية بين الوحدات العسكرية المعادية؛ لإرباكها وشل سيطرتها على قواتها وأسلحتها.

وفي عام 1904 قصفت السفينتان اليابانيتان الحربيّتان "كاسوفا ونيشين" القاعدة البحرية الروسية في ميناء "آرثر" Arthur، وكانت معهما سفينة صغيرة تصحح التيار باستخدام الراديو "اللاملكي"، وسمع أحد عمال "الإشارة" الروس، بالمصادفة، تعليمات تصحيح التيار، فاستخدم جهاز إرساله اللاسلكي في إعاقه الاتصال الياباني بالضغط على مفتاح الإرسال على تردد الشبكة اليابانية نفسها، مما عطل بلاغات تصحيح التيار من أن تُبلّغ لمدفعية السفينتين؛ وهكذا، لم ينتج عن هذا القصف البحري سوى إصابات طفيفة، لعدم دقة التيار في إصابة أهدافها. وحتى عام 1905، وخلال المعارك بين السفن اليابانية والروسية، استخدمت السفن الروسية الأسلوب نفسه ضد الشبكات اللاسلكية اليابانية، وانعكس ذلك في أن السفن الروسية استطاعت إخفاء اتصالاتها، قدر الإمكان، من طريق تقليل فترات استخدام اللاسلكي لأقل فترة ممكنة، وبأقل قدرة إشعاع لاسلكي تحقق الاتصال المطلوب، وكانت السفن الروسية تتصت وتراقب الإرسال اللاسلكي الياباني، ثم تشوش عليه أثناء القصف بهذا الأسلوب نفسه. وفي عام 1906 استطاع مكتب معدات البحرية الأمريكية من استحداث جهاز تحديد اتجاه لاسلكي لخدمة الملاحة البحرية في البحر، وهو ما يعرف باسم "المنارة اللاسلكية" لإرشاد السفن، وتحديد مواقعها، وخطوط سيرها، مما كان له أثر كبير في محاللات الحرب الإلكترونية فيما بعد.

الحرب الإلكترونية في الحرب العالمية الأولى

في بداية الحرب العالمية الأولى، في أغسطس 1914، قبل أن تدخل بريطانيا الحرب إلى جانب بلجيكا وفرنسا، ضد ألمانيا، والنمسا، مرت سفينتان حربيتان بريطانيتان، بجوار السفن الألمانية في بحر المانش، ولم تحاولا الاشتباك مع السفن الألمانية. إلا أن أدميرال الأسطول الألماني "إرنست كينج"، أوضح أن هاتين





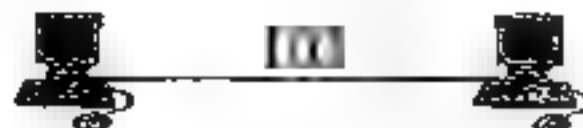
السفينتين البريطانيتين، نفذتا عمليات التنصت اللاسلكي على الاتصالات اللاسلكية للسفن الألمانية، وذلك عندما حاولتا التشويش على الاتصالات اللاسلكية الألمانية، بهدف اختبار كفاءة أعمال الحرب الإلكترونية لديها في التدخل والشوشرة اللاسلكية على الشبكات اللاسلكية الألمانية.

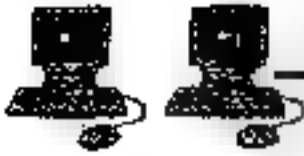
وأثناء العمليات البحرية التالية في الحرب العالمية الأولى، كان التشويش على الاتصالات اللاسلكية يستخدم من حين إلى آخر، ولكن وُجد أنه، لكي تنفذ التشويش على أي اتصال لاسلكي، كان لا بد أن تسبق عملية التنصت هذا الاتصال، الأمر الذي تبين منه في أحيان كثيرة، أهمية المعلومات التي يتبادلها الجانب المعادي، والتي يمكن الحصول عليها، معرفة نواياه المستقبلية.

ومن هنا ظهرت أهمية أعمال الاستطلاع اللاسلكي على شبكات العدو اللاسلكية، بهدف الحصول على المعلومات، كما أصبحت الوحدات البحرية على دراية بأن استخدام اللاسلكي أكثر مما ينبغي، يمكن أن يفصح عن حجم كبير من المعلومات المفيدة للعدو، حتى مع استخدام الكود والشفرة في الاتصالات اللاسلكية

ولهذا السبب، أكد القادة على أهمية بقاء الراديو "اللاسلكي" صامتاً صكلاً أمكن ذلك، وتقليل تبادل الإشارات إلى الحد الأدنى عندما لا يكون آمناً، أي بمجرد أن تكون السفن الحربية في مرمى بصر العدو، فكان لا يسمح للقادة باستخدام الراديو "اللاسلكي" بحرية حتى لا يلتقطه الجانب المعادي، وكان يستعاض عنه، في تحقيق الاتصال، باستخدام الإشارات المرئية "التأشير المنظور"

بعد ذلك ظهرت أهمية تحديد مواقع المحطات اللاسلكية المعادية، التي تدل على أماكن تركز القوات المعادية، وبالتالي يمكن التنبؤ المبكر بالتهديد، وكذلك لتوجيه أعمال الشوشرة ضدها بدرجة تركيز مناسبة في التوقيت المناسب، ففي عام 1915، استغلت البحرية البريطانية الفكرة الأمريكية في إنشاء جهاز تحديد اتجاه الإشعاع اللاسلكي الصادر من جهاز إرسال أي سفينة تستخدم الاتصال اللاسلكي وهي في عرض البحر، والذي يمكن باستقباله تحديد موقع





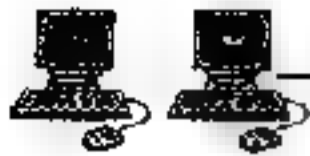
هذه السفينة "نظام المنارة اللاسلكية"، وعلى ضوء ذلك، بدأت البحرية الملكية البريطانية، بتركيب سلسلة من محطات تحديد الاتجاه اللاسلكي بطول الساحل الشرقي لإنجلترا، حيث أمكنها تحديد موقع أي سفينة أو طائرة منطلقة في بحر الشمال وعندما دخلت أمريكا الصراع في أبريل 1917، انضم الأسطول الحربي الأمريكي مع الأسطول البريطاني، الذي كان يمتلك أجهزة لاسلكية متقدمة، وكانت بعض قطع الأسطول تحمل أجهزة تحديد اتجاه من نوع 995، أثبتت كفاءة كبيرة في تحديد مواقع السفن المعادية التي كانت تتنصت على اتصالاتها اللاسلكية، وتحدد مواقعها، وتتبعها، ثم تدمرها.

ومع تزايد الاهتمام بالاتصالات اللاسلكية من الجو إلى الأرض من خلال إرسال تقارير الاستطلاع التكتيكي عن أرض المعركة، أو لتصحيح نيران المدفعية في إصابة أهدافها، ولأهمية المعلومات المتبادلة على هذه الشبكات؛ كان غالباً، ما يشوش عليها، لحرمان الجانب المعادي من الحصول على معلومات عن الأهداف المطلوب تدميرها، وكذلك حرمانه من أن يصحح نيران مدفعيته، وإصابة الأهداف بدقة

الحرب الإلكترونية بين الحرب العالمية الأولى والثانية

أجرت عدة دول تجارب على قيام الطائرات بتوجيه القنابل لاسلكياً. وفي ثلاثينيات من القرن العشرين الميلادي تطورت أجهزة الإرسال بدرجة كبيرة، وأنتجت أجهزة استقبال ذات حساسية عالية، وهوائيات دقيقة التوجيه، وهو ما أدى إلى التفكير في التداخل اللاسلكي لإفشال أعمال التوجيه. وفي هذا الوقت، بدأت التطبيقات العملية للظواهر المكتشفة عام 1900، صدى الصوت؛ إذ كان عندما يرفع الصوت، ويسمع صدى في الإجابة، يعرف أن الصوت وصل حائطاً بعيداً، أو حاجزاً، ولا بد أنه انعكس من المكان نفسه وهكذا، بدأ تطبيق تحديد المكان لأي جسم متحرك، مثل سفينة في البحر، إذ يمكن من تحديد مسافة تحركها في زمن محدد، وحساب سرعتها؛ ففي البداية،





يحدد مكان الهدف المتحرك وتوقيته في موقع ما ، ثم بعد فترة زمنية محددة ، يعاد تحديد مكان الهدف وتوقيته في موقع آخر ، وبحساب المسافة التي تحركها الهدف ، بين الموقعين الأول والثاني ، والزمن الذي استغرقه في قطع هذه المسافة ، تحدد سرعة الهدف من المعادلة الآتية:

$$\text{السرعة} = \frac{\text{المسافة}}{\text{الزمن}}$$

وقد طبق العاملون في معمل أبحاث البحرية الأمريكية ذلك ، خلال تجارب اكتشاف الرادار عام 1922 . وفي عام 1934 ، كان جهاز الرادار الأمريكي ، قادراً على اكتشاف الطائرات على مسافة 50 ميلاً؛ وفي هذه الفترة ، كان هناك عمل مشابه ، ينفذ في بريطانيا وألمانيا . وبحلول شهر يونيه 1935 ، أنتج أول رادار نبضي للبحرية البريطانية ، يمكنه كشف الأهداف حتى مدى 17 ميلاً . وفي مارس 1936 ، أنتج جهاز مماثل معدل بمدى كشف 75 ميلاً . وهكذا ، تطور تصنيع الرادارات على المسرح الأوروبي ، وفي الولايات المتحدة الأمريكية .

الحرب الإلكترونية في الحرب العالمية الثانية

وحتى ديسمبر 1938 ، تمكنت الدول الأوروبية من إنتاج رادارات ، ذات مدى كشف راداري 100 ميل عن الطائرات المعادية توفر زمن إنذار لأكثر من نصف ساعة ، عن هجوم قاذفات القنابل المعادية ، فضلاً عن إنتاج رادار بحري ، يوفر مدى كشف راداري 15 ميلاً عن القطع البحرية المعادية .

ومنذ أكتوبر 1935 ، كلف مسؤول البرنامج البريطاني لتطوير الرادار بدراسة إمكانية التشويش على أجهزة الكشف الراداري؛ إذ بدأت التجارب ، وأمكن تحقيق نتائج إيجابية في عام 1938 ، وفي عام 1939 . كما بدأت في إنجلترا دراسة إمكانية تشغيل عمال الرادار على أجهزتهم ، في ظل قيام العدو بأعمال الإعاقة والتشويش ، على الرادارات الإنجليزية .

ومع تزايد الانتصارات الألمانية في فرنسا وهولندا وبلجيكا ، في صيف 1940 ، والإجلاء السريع للقوات البريطانية من الجزء الرئيسي من أوروبا ، وتزايد





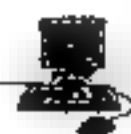
إمكان دخول الولايات المتحدة الأمريكية الحرب إلى جانب الحلفاء، بدأت واشنطن، في سرية تامة، بتعبئة الهيئات العسكرية الصناعية والعلمية وتنظيمها، لخدمة الحرب الإلكترونية.

أما الإنجاز الكبير الذي حدث بعد ذلك، هو أنه، بعد سقوط فرنسا، هرب العالم "موريس دولورين" إلى الولايات المتحدة الأمريكية، ومعه ثلاثة من زملائه الذين كانوا يعملون في نوع جديد من أجهزة تحديد الاتجاه ذات التردد العالي للبحرية الفرنسية، وبدعوا العمل في مختبر الاتصالات اللاسلكية الفيدرالي في "أماج نسيه" بولاية "كونج أيلاند" Long Island، وسرعان ما قاموا بتشغيل نموذج متطور لتحديد الاتجاه اللاسلكي يعمل على الشواطئ، ثم طوروا جهازاً آخر للعمل بالسفن الحربية، دخل الخدمة في القوات البحرية بعد ذلك.

ومنذ أوائل ديسمبر 1941، وقبل دخول الولايات المتحدة الأمريكية الحرب مباشرة، أُنشئت رادارات متقدمة منها SCR-270، ثم SCR-271، وذلك بزيادة حيز تردد لها، ركبت فيما بعد، بالسفن الحربية، وحاملات الطائرات، والطرادات، بما أدى إلى التغلب على أعمال الاستطلاع والإعاقة الرادارية.

وفي الوقت نفسه، كانت الإجراءات المضادة للرادارات تعبر سيراً حسناً، مثل مستقبل التحذير الرادار (جهاز استقبال راداري، يركب في الطائرة أو في القطعة البحرية، يمكنه استقبال نبضات الرادار المعادي، فيعطي إنذاراً لقائد الطائرة/ القطعة البحرية أنه أصبح مكتشفاً رادارياً، وعليه تنفيذ التدابير الإلكترونية لتجنب هذا الكشف). من الرادارات المعادية Radar Warning Receiver: RWR من نوع P-540، والذي تطور، بعد ذلك، إلى ما أطلق عليه P-587، والذي أقر في مختبر الطاقة الإشعاعية.

وهكذا، زاد التنافس بين القوات المتحاربة في المحيط الأطلسي والمحيط الهادي، مما ساعد على التطوير المستمر في معدات الحرب الإلكترونية وأعمالها، حتى وصلت إلى ما هي عليه الآن، في ظل التطور الهائل لتكنولوجيا الإلكترونيات





وهكذا استمر الصراع الدائر للحصول على التكنولوجيا المتقدمة لإنشاء أحدث النظم الإلكترونية اللازمة للسيطرة وإدارة النيران، وللمعاونة في إدارة أعمال القتال. وكان يتبعها دائماً العمل الدائم في مراكز الأبحاث للوصول إلى أكثر المعدات الخاصة بالحرب الإلكترونية تعقيداً من وسائل للاستطلاع والإمهقة على هذه المعدات المتقدمة، التي يتم إنشاؤها. ثم يأتي دور اختيار هذه المعدات الجديدة في مجال الحرب الإلكترونية ليتم إنزالها إلى ساحة القتال، لمعرفة تأثيرها، ثم تجرى أعمال التطوير مرة أخرى على ضوء ما يدرس من مزاياها وعيوبها. ظهر ذلك واضحاً في حروب ما بعد الحرب العالمية الثانية: "كوريا - فيتنام - حرب 1967 - حرب 1973 - هوكلايد - سهل البقاع - خليج سرت - ثم حرب البلقان.

أسلحة الحرب الإلكترونية

مهما كان نوع الحرب المعلوماتية - ضد فرد، مؤسسة، أو دولة - فلا بد من وجود أسلحة تستخدم لتنفيذ هذه الحرب ومن هذه الأسلحة:

1 - فيروسات الحاسوب

هي برامج خارجية صُنعت عمداً بفرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات. أي أن الغرض منها هو إلحاق الضرر بحاسوب آخر أو السيطرة عليه، وتتم كتابتها بطريقة معينة وقد تستخدم الفيروسات لتعطيل شبكات الخدمات والبنية التحتية لطرف المستهدف كأن يتم عن طريقها إحداث فشل في شبكة الاتصالات لدولة ما كما حدث مع نظام شركة AT&T الأمريكية في 15 يناير سنة 1990 ميلادي^{5,7,8}.

2 - الديدان Worms

هي برامج صغيرة مستقلة لا تعتمد على غيرها وتتكاثر بنسخ نفسها عن طريق لشبكات صممت للقيام بأعمال تخريرية كأن تعمل على قطع الاتصال بالشبكة أو سرقة بعض البيانات الخاصة بالمستخدمين أثناء تصفحهم للإنترنت،





تمتاز بسرعة الانتشار ويصعب التخلص منها نظراً لقدرتها الفائقة على التلون والتناسخ والمراوغة. غالباً عندما تستخدم في حروب المعلومات تستهدف الشبكات المالية التي تعتمد على الحاسوب، مثل شبكات البنوك.

3 - أحصنة طروادة Trojan horses

هي شفرة أو برنامج صغير مخفي في برنامج كبير من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية كأن يعمل على نشر دودة أو فيروس. وهو مبرمج بمهارة عالية إذ لا يمكن اكتشاف وجوده؛ حيث يعمل دائماً على مسح آثاره التي لا تحمل صفة تخريرية وغالباً ما يعمل على إضعاف قوى الدفاع لدى الضحية ليسهل اختراق جهازه وسرقة بياناته كأن يقوم مثلاً بإرسال بيانات عن الثغرات الموجودة في نظام ما، وكذلك إرسال كلمات المرور السرية الخاصة بكل ما هو حساس من مخزون معلومات الطرف المستهدف.

4 - القنابل المنطقية logic bombs

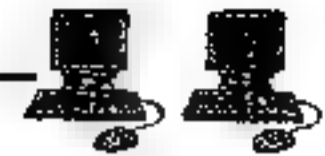
تعد نوع من أنواع أحصنة طروادة حيث يزرعها المبرمج داخل النظام الذي يطره وقد تكون برنامجاً مستقلاً وتُصمم بحيث تعمل عند حدوث أحداث معينة أو تحت ظروف معينة أو لدى تنفيذ أمر معين. وتؤدي إلى تخریب أو مسح بيانات أو تعطيل النظام لطرف المستهدف.

5 - الأبواب الخلفية backdoors

هي ثغرة تُترك عن عمد من قبل مصمم النظام؛ لكي يستطيع الدخول إلى النظام عند حاجته لذلك. وتجدر الإشارة إلى أن كل البرامج والنظم التي تنتجها الولايات المتحدة الأمريكية تحتوي على أبواب خلفية تستخدمها عند الحاجة، وهو ما يمكن هيئات وأركان حرب المعلومات من التجوال الحر داخل أي نظام لأي دولة أحسية.

6 - الرقائق chipping

ممن الممكن أن تحتوي بعض الرقائق على وظائف غير متوقعة أو معروفة كما في البرامج والنظم حيث يمكن للدوائر المجهزة التي تشكل هذه الرقائق أن



تحتوي على وظائف إضافية أثناء تصنيعها، لا تعمل في الظروف العادية، إلا أنها قد تعلن العصيان في توقيت معين، أو بالاتصال بها عن بعد؛ حيث يمكن أن تستجيب لتردد معين لبعض موجات الراديو، فتشل الحياة في مجتمع أو دولة ما..

7 - الماكينات والميكروبات فائقة الصغر

ويطلق عليها (Nano machines and Microbes)، وهي عكس الفيروسات، حيث أنها تصيب عتاد النظام (Hardware) فالـ (Nano machines) عبارة عن (robots) فائقة الصغر قد تنتشر في مبنى نظام معلوماتي في دولة معادية أو منافسة؛ حيث تتمشى في الردهات والمكاتب حتى تجد حاسباً آلياً، وتدخل إليه من خلال الفتحات الموجودة به، لتبدأ عملها بإتلاف الدوائر الإلكترونية.

أما الميكروبات (Microbes) فمن المعروف أن بعضاً منها يتغذى على الزيت، فماذا لو تم تحويلها جينياً لتتغذى على عنصر السيليكون (silizium) (المكون الهام في الدوائر الإلكترونية)؟ إن هذا يعني تدمير وإتلاف الدوائر الإلكترونية في أي معمل يوجد فيه حاسبات آلية أو حاسب خادم (server) لموقع على الإنترنت، أو مبنى هام أو حساس يدار بالكمبيوتر، أو حتى مدينة بأسرها عن طريق إتلاف دوائر التحكم الإلكترونية فيه.

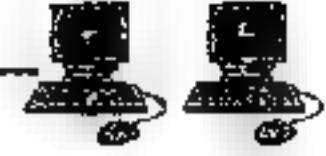
8 - الاختراق المروحي الإلكتروني

في الماضي تم استخدام التشويش الإلكتروني لعرقلة الاتصال وربما قطعه بحيث لا يتمكن الطرف المستهدف من إرسال واستقبال المعلومات. ولقد تم تطوير هذه الخطوة ليصبح بدلاً من عرقلة الاتصال استبدال المعلومات وهي في طريقها إلى المستقبل بمعلومات غير صحيحة.

الحرب الإلكترونية المستقبلية

أكدت التقارير الصحفية أن الصين تضع خطة لفرض "هيمنة إلكترونية" على خصومها العالميين بحلول عام 2050 خاصة الولايات المتحدة وبريطانيا وألمانيا وروسيا وكوريا الجنوبية.





ودكرت صحيفة "التايمز" البريطانية عن مصادر في البنتاجون أن الصين تجهز لضربات معلوماتية تحسباً لهجوم عسكري أمريكي، وأن قراصنة الكمبيوتر من الجيش الصيني وضعوا خطة لتعطيل أسطول حاملات طائرات أمريكية عن طريق هجوم معلوماتي.

وعلى عكس ما كان معروفاً قديماً من أن الضربة الجوية تعد هي عنصر المبادرة في أي حرب، ومنها بالطبع حرب أكتوبر 73 الذي حقق فيها الجيش المصري الانتصار على الجيش الإسرائيلي وكان الطيران هو كلمة السر فيها، إلا أن اليوم ووفقاً لما جاء في تقرير البنتاجون فإن الجيش الصيني يعتبر "الهجمات المعلوماتية" هي "وسيلة كسب المبادرة" في المراحل الأولى من أي حرب، حيث ترغب الصين في شن هجمات العدو المالية والعسكرية والاتصالية في المراحل المبكرة من النزاع.

في الجيش الصيني دليل افتراض لحرب إلكترونية ولتشويش، بعد أن قاموا بدراسة إرشادات وضعها حلف الأطلسي والولايات المتحدة حول الأساليب العسكرية. لأغراض عسكرية وأظهرت الصحيفة أن البنتاجون سجل أكثر من 79 ألف محاولة قرصنة خلال عام 2005 نجح منها نحو 1300 محاولة.

يأتي ذلك بعد أن وجهت كل من ألمانيا والولايات المتحدة وبريطانيا أصابع الاتهام إلى الصين، بشأن هجوم قراصنة على شبكاتهم الإلكترونية لتحقيق أغراض عسكرية.

فقد اتهم مسئولون أمريكيون الجيش الصيني بشأن هجوم قرصنة ناجح على أجهزة الكمبيوتر في مبنى وزارة الدفاع الأمريكية في يونيو الماضي.

وقد نقل راديو هيئة الإذاعة البريطانية "بي بي سي" عن هؤلاء المسئولين قولهم أنهم تأكدوا من أن الجيش الصيني هو مصدر الهجوم على الشبكة، والذي أدى إلى تدمير جزء من نظامها. فمنذ شهور قليلة تعرضت وزارة الدفاع الأمريكية "البنتاجون" لهجوم كاسح للـ "هاكرز"، حيث قام قراصنة بشأن هجوم على ثلاثة عشر جهازاً مركزياً يتحكم بتدفق المعلومات على شبكة الانترنت على مستوى





العالم، وتمكنوا من تعطيل ثلاثة أجهزة والسيطرة عليها بشكل كامل طوال اثنتي عشر ساعة، في أكبر عملية تشهدها الشبكة منذ عام 2002.

القراصنة نجحوا في الثهور الماضي في اختراق شبكة وزارة الدفاع الأمريكية والبريطانية.

وقد تركز الهجوم الذي تمكن الخبراء من مواكبته بشكل عاجل دون أن يشعر به معظم مستخدمي الإنترنت على أجهزة شركة ultra DNS، وهي الشركة التي تدير وتظم جميع خطوط الشبكة التي تنتهي بالرمز "org" وهما اكتفت الشركة بالقول أنها لاحظت حركة "غير عادية" ضمن النظام، تردد أن الهجوم طال عدداً من الخوادم الرئيسية التي تسيطر تدفق المعلومات عالمياً، والتي تعود ملكية بعضها إلى وزارة الدفاع الأمريكية وأجهزة الرقابة على الإنترنت.

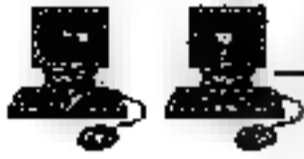
ووصف المراقبون الهجمة بأنها كانت "قوية بصورة غير اعتيادية"، غير أن خبراء المعلوماتية حول العالم نجحوا في احتوائها، بعدما بذلوا مجهوداً كبيراً ليحافظوا على كفاءة بعض خطوط الشبكة الحيوية، التي اتخمت بفيض هائل من المعلومات.

ونجح القراصنة في اختراق نظام البريد الإلكتروني غير السري لوزارة الدفاع الأمريكية "البنتاجون"، مما أدى إلى تعطيل الخدمة لنصف الطاقم لخاص بوزير الدفاع روبرت جيتس.

دودة طروادة وعشبة زيارة المستشار الألمانية أنجيلا ميركل لبكين نهاية العام الماضي، هانت مجلة "دير شبيجل" الألمانية أن كمبيوترات مكتب المستشار وثلاث وزارات أصيبت بـ "دودة" من نوع "حصان طروادة" أو "تروجان".

ولم يحدد المقال الجهة المسؤولة أو مصدر الدودة، لكنها أشارت إلى أن الاستخبارات المحلية الألمانية تعتقد أن مجموعة مرتبطة بالجيش الصيني ربما تكون وراء الاختراق المزعوم، وكانت وزارة الدفاع الأمريكية قد حذرت في مطلع العام الحالي من أن الجيش الصيني يشدد على اختراق أنظمة الكمبيوتر بوصفه سلاحاً دفاعياً





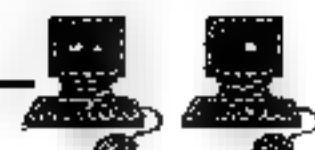
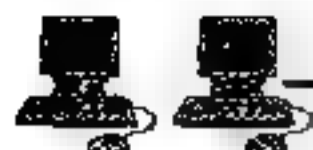
اعتراف بريطاني وبهذا اكتمل الضلع الثالث في مثلث ضحايا حرب القرصنة بعد انضمام بريطانيا هي الأخرى إلى الولايات المتحدة وألمانيا بعد تعرض شبكات الكمبيوتر الخاصة بالحكومة البريطانية هي الأخرى لمثل هذه الهجمات. ونقلت صحيفة الجارديان البريطانية عن مسؤولين بريطانيين قولهم أن القراصنة احترقوا شبكة وزارة الخارجية وغيرها من الوزارات الكبرى، مشيرة إلى أن وزارة الدفاع البريطانية رفضت تأكيد ما إذا كانت شبكتها تعرضت للاختراق من قبل القراصنة الصينيين. وأضاف المسؤولون أن حادثاً وقع العام الماضي وأدى إلى إغلاق جزء من نظام الحاسوب في مجلس العموم البريطاني، وتبين أنه من عمل عصابة صينية منظمة من قراصنة الكمبيوتر.

وأشارت الصحيفة إلى أن مسؤولي الأمن والدفاع البريطانيين يتعاملون بتحفظ مع المسألة، غير أنهم اعترفوا بأن بعض الوزارات وقعت ضحية لمصابة قرصنة الكمبيوتر الصينية، والتي وصفها أحد الخبراء بأنها "مشكلة تتطور باستمرار" أشعل الإنترنت مؤخراً شرارة البدء في إصرار السادس من أبريل بمصر، وكان المحرك الأساسي لإذكاء الحماس لدى المواطنين، وقد أبرز هذا الدور إشكالية استغلال بعض الجهات لهذه الميزة لتحقيق أهداف بعيدة تماماً عن الغرض الرئيسي لظهور هذه الوسائل، فبانت نظرية المؤامرة هي المفسر الرئيسي للأحداث، وفور الانقطاع الفاضل للإنترنت في الشرق الأوسط أكد الخبراء أن قطع هذه الكابلات لم يكن مصادفة، لندخل بذلك مرحلة جديدة للحرب الإلكترونية.

كما ظهرت مؤخراً بوادر اقتحام الإنترنت المجال العسكري وهو ما اعتبر نوعاً جديداً من الحروب تحولت عن شكلها التقليدي لتتخذ شكلاً آخر إلكترونياً تحركه ممتلح الكيبورد بدلاً من زناد المدافع والأسلحة، وتعتمد على الفيروسات والتروجان بدلاً من الطلقات والدانات.

زادت في الآونة الأخيرة وتيرة الأحداث المتمثلة بالاعتداءات الإلكترونية التي تستهدف مواقع اقتصادية وتكنولوجية وحكومية حساسة ويكون أبطالها مجموعة من هواة القرصنة تحت عنوان "الهكرز" يتنوع هدفهم المعلن بين السرقة والانتقام





وإثبات الوجود وفي أحيان كثيرة يكون "التخريب" المقصود والمدعوم من دول معينة تحاة دول أخرى في حرب الكترونية "بالنيابة" شملت أضرارها أغلب دول العالم التي باتت تعتمد على الانترنت في تسير معظم مجالاتها الحيوية اعتماداً وثيقاً حيث بات أي تهديد يمس هذا الجانب لديها من الممكن أن يؤدي إلى انهيارات كبيرة داخل مؤسساتها المهمة.

إن الأمثلة على ذلك أصبحت كثيرة ويكفي ذكر الفيروس الذي أصاب المفاعل الإيراني ونجح في إخراجه عن الخدمة مؤقتاً بعد أن تسبب في ضرار قوية حيث اتهمت إيران الولايات المتحدة وإسرائيل في الوقوف خلف هذا الهجوم الإلكتروني. كما أن العديد من المواقع الإلكترونية الرسمية للولايات المتحدة الأمريكية نفسها تعرضت إلى هجوم أيضاً مما حدا بوزارة الدفاع الأمريكية إلى التصريح حول تقديمهم لدراسة تقتضي استخدام القوة "بمختلف أشكالها" في حال تعرضت مصالح الولايات المتحدة الأمريكية إلى الخطر نتيجة هذه الهجمات، مما يفتح الباب على مصراعية أمام حرب جديدة الملامح.

الأهداف المعادية للحرب الإلكترونية

هي الأهداف المطلوب أن تتعامل معها الحرب الإلكترونية بأعمال الاستطلاع، والإعاقة الإلكترونية، ويمكن أن نوجز أهم هذه الأهداف فيما يلي:

1. محطات الاتصال اللاسلكي، واللاسلكي متعدد القنوات، والميكروويف

2. أنظمة الرادار العسكرية

أ. للإنذار وتوجيه النيران

ب. للإنذار والمراقبة الساحلية.

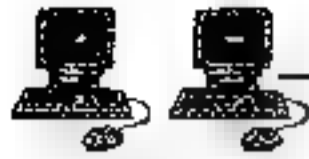
ج. للتوجيه لمراكز السيطرة الجوية.

د. لقيادة نيران المدفعية وتصحيحها.

هـ. لمراقبة التحركات الأرضية.

3. نظم الكشف والتوجيه الكهرومصرية "تليفزيوني، وحراري، وليزري، وبصري".





مجالات الحرب الإلكترونية

إذا كان البر، والبحر، والجو، والفضاء الخارجي، هي المسارح التقليدية للحرب، فيُعدّ حيز المجال الكهرومغناطيسي - مجال انتقال الموجات الترددية بأنواعها - وأطوالها الموجية المختلفة - هو المسرح الحقيقي للحرب الإلكترونية؛ إذ تتنازع الأطراف المتحاربة على استغلال هذا المجال لمصلحته.

تمتد مسارح الحرب الإلكترونية من قاع المحيطات حتى الطبقات العليا لفضاء الخارجي؛ إذ يستخدم فيها مختلف النظم الإلكترونية: المراقبة والكشف، والقيادة والسيطرة، والإعاقة والخداع، ورصد الأهداف، وتوجيه الأسلحة، وجميع هذه النظم تستخدم نظم تحليل الإشارات Signal Processing في تحليل الموجات المنعكسة من نبضات التردد الموجي للمجال الكهرومغناطيسي.

نماذج من حرب الفضاء الإلكتروني

في يوم آت، سوف يحدد المؤرخون العسكريون تاريخ اندلاع أول حرب فضاء إلكتروني. وحتى حين ذلك التاريخ، يمكن القول إن الفيروس ستكسنت (Stuxnet) قد مثل في العام 2010 أول ابتلافة غير رسمية لهذه الحرب.

وقد استخدم هذا الفيروس في الهجوم على المنشآت النووية الإيرانية، واستطاع أن يتغلغل في أنظمتها، مستفيداً من فجوات لم تكن معروفة حتى ذلك الوقت في نظام ويندوز. ويعتقد أن ستكسنت قد أصاب نحو 100 جهازاً من أجهزة الطرد المركزي المستخدمة في تخصيب اليورانيوم.

كما اعتبر الفيروس فليم (Flame) أكثر ضرراً من ستكسنت، بيد أنه لا يستهدف تدمير الأجهزة، بل سرقة بياناتها. وقد وجه الفيروس فليم، في مايو/أيار 2012 لأجهزة كمبيوتر خاصة بعدد من المسؤولين الإيرانيين.

وفي 15 أكتوبر/تشرين الأول 2012، رصدت نسخة جديدة من هذا الفيروس في أجهزة كمبيوتر، في كل من إيران ولبنان وفرنسا. وقد أطلق على هذه





النسخة اسم "ميني فليم". وقدر عدد الهجمات التي تمت بواسطةها في أنحاء العالم بما بين 50 و60 هجوما.

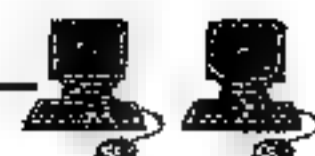
في الجهة المقابلة، تعتقد الولايات المتحدة أن إيران ربما تقف خلف عدد من الهجمات الإلكترونية، التي استهدفت مؤسسات مالية أميركية، في أكتوبر/تشرين الأول 2012. وكانت إيران قد أعلنت في العام 2011 عن بناء وحدة عسكرية إلكترونية خاصة بها.

ورغم ذلك، تشير تقديرات الهيئات الأميركية إلى أن قدرات حرب الفضاء الإلكتروني لدى إيران لا تزال في بداياتها، وهي لا تقارن بتلك الموجودة لدى الصين وروسيا، اللتين تقفان، حسب واشنطن، خلف عدد كبير من الهجمات على الشركات والوكالات الحكومية الأميركية.

وتحدثت الولايات المتحدة عن مئات آلاف الهجمات الإلكترونية التي تشن عليها يوميا، وتعرضت بعض المؤسسات الأميركية في الأشهر الأخيرة لما يسمى بهجمات منع الخدمة، حيث يستحدم متسللون قدرا كبيرا من الرسائل الواردة لتأخير المواقع الإلكترونية أو تعطيلها. وقد زادت هذه الهجمات في الربع الثالث من العام 2012 بنسبة 88٪، قياسا بما كانت عليه في الفترة نفسها من العام 2011. وفي 19 أكتوبر/تشرين الأول 2012 قال وزير الدفاع الأميركي ليون بانيت إن بلاده تواجه "تهديدا عسكريا مستجدا تماما"، هو حرب الفضاء الإلكتروني. وعليها أن توليه انتباهها الشديد، "لأنه ساحة حرب المستقبل".

ويسمى البنتاغون حاليا لبناء خريطة مفصلة للفضاء الإلكتروني العالمي، تضم مليارات المواقع الإلكترونية، وتعمل على تحديث نفسها تلقائيا. كما طلب من القوات الجوية تقديم مقترحات لإدارة حرب الفضاء الإلكتروني، بما في ذلك القدرة على شن هجمات على أجهزة الكمبيوتر فائقة السرعة، وصد الهجمات الانتقامية. وتتكون قاعدة الاتصالات العالمية للقوات العسكرية الأميركية، في الوقت الراهن، من 15 ألف شبكة إلكترونية، وسبعة ملايين جهاز حاسوب، موزعة عبر





المئات من المنشآت، وفي العشرات من البلدان. وهناك أكثر من 90 ألف شخص يعملون بدوام كامل للحفاظ على هذه القاعدة التقنية.

وفي الغالب، تتحفظ الولايات المتحدة على الحديث عن خططها الخاصة بحرب الفضاء الإلكتروني، وذلك خشية إثارة سباق عالمي في هذا المجال. بيد أنها تبحث حالياً فكرة الإعلان عن قدراتها الهجومية الإلكترونية لتكون عامل ردع في مواجهة الأعداء المحتملين أو الافتراضيين.

ولم تستخدم واشتعلن حتى اليوم عبارة هجوم في حديثها المقتضب عن برنامجها لخاص بحرب الفضاء الإلكتروني. وتركز بدلا من ذلك على عبارات مثل الدفاع عن مصالح الأمة، والتصدي للنمط الجديد من الأخطار.

وجاء التعليق الأكثر إثارة للانتباه من الوزير بانيتا في 11 أكتوبر/تشرين الأول 2012، حين أوضح أن الولايات المتحدة قد تستخدم قدراتها الهجومية في حرب الفضاء الإلكتروني إذا اكتشفت أن هناك تهديدا إلكترونيا وشيكاً من شأنه التسبب في قتل مواطنين أميركيين، أو إلحاق أضرار مادية جسيمة بالبلاد.

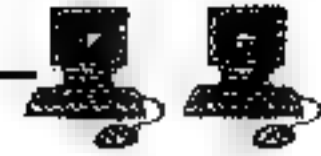
نماذج من الحرب الدولية الإلكترونية

تتنوع وتعدد أشكال الحروب التي خاضتها ولا زالت تخوضها العديد من الدول نذكر منها:

- حرب الهاكرز العظمى

أشهر تلك الحروب على الإطلاق هي (حرب الهاكرز العظمى) التي دارت رحاها بين عامي 1990 و 1994 بين فريقين من الهاكرز المحترفين: LOD & MOD في عام 1984 أنشأ ليكس لوثر مجموعة أسماها LOD كان هدفها التلويح إلى حواسيب الآخرين والعبث بها، كانت تلك المجموعة تُعتبر من أدكى مجموعات الهاكرز إلى أن ظهرت جماعة أخرى أسماها شخص يُدعى < فيبر > وأطلق عليها MOD، ثم حدثت منافسة شديدة بين الفريقين أشعلت ما يُعرف بحرب الهاكرز العظمى حيث سُمي كل فريق لاختراق حواسيب الآخر، ثم كانت





النهاية غير سارة حيث انتهت بالقبض على فيبر، وما لبثت الساحة أن شهدت ظهور أشخاص وجهات أخرى أكثر مهارة وأكثر شهرة، لعل أشهرهم على الإطلاق كيفن ميتيك.

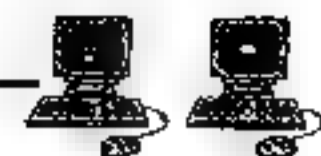
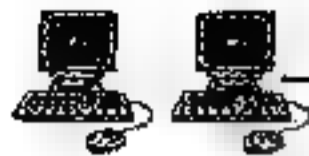
يُعتبر (كيفن ميتيك) أشهر هacker في التاريخ، فقد قام بسرقات كبيرة دوخت "إف بي أي" ولم يستطع خبراءها تحديد هويته في أغلب سرقاته، لكن في أحد المرات وأثناء اختراقه شبكة الكمبيوترات الخاصة بشركة Digital Equipment Company تم تتبعه وكشفه والقبض عليه وسجنه لمدة عام وبعد خروجه من السجن كان أكثر ذكاء فكانوا لا يستطيعون ملاحقته فقد كان كثير التغير من شخصيته كثير المراوغة في الشبكة ومن أشهر جرائمه سرقة الأرقام الخاصة بـ 2000 بطاقة إئتمان والتي كانت آخر جريمة له تم القبض بعدها عليه وسجنه لمدة عام وقررت الإف بي أي أن كيفن خطير ولا توجد شبكة لا يستطيع اختراقها.

ظهرت أصوات تطالب الحكومة بالإفراج عن كيفن وظهرت جماعات تقوم بعمليات قرصنة باسم كيفن من بينها قرصنة موقع جريدة نيويورك تايمز التي ظهرت شاشتها متغيرة كثيراً في مرة من المرات وظهرت كلمات غريبة تعلن للجميع بأن هذه الصفحة تم اختراقها من قبل كيفن ميتيك، ولكن تبين بعد ذلك بأنه أحد الهاكرز الهواة المناصرين لميتيك في عام 2000 تم الإفراج عنه بشرط ألا يستخدم الكمبيوتر إلا بعد موافقة مكتب المراقبة التابع له.

هناك العديد من الحالات التي تم رصدتها لخروقات قام بها الهاكرز في الفترة الممتدة بين 1983 و 2002 نذكر منها:

1983 تم القبض على ستة مراقبين كونوا جماعة عرفت باسم الـ <414>، قاموا بحوالي 60 اختراقاً لأنظمة الكمبيوتر، منها المعهد القومي في لوس أنجلوس في ميلواكي، وقد تم إطلاق أحدهم بعد أن حصل على الحصانة لشهادته، وعلقت العقوبة بالنسبة للخمسة الباقين.





1985 اثنان من الصحفيين أسسا مجلة phrack في سانت لويس، تقدم

معلومات عن اختراق النظم والحواسيب.

1987 مراهق عمره 17 عاما لم يكمل دراسته الثانوية ويدعي هيربرت رن،

وعرف فيما بعد بصقر الظل، اعترف بقيامه باختراق أجهزة الحاسب لشركة

AT&T للاتصالات في بدمنستر، من غرفة نومه بشيكاغو، وهو يعد من أوائل

الذين حوكموا بتهمة الاحتيال لاختراق نظم الكمبيوتر.

1988 روبرت موريس، خريج جامعة كورنيل، قام بتطوير أقوى شبكية

تستغل الثغرات التي بأنظمة يونكس، وانتشرت في حوالي 6000 جهاز وهو

مايساوي عشر أجهزة الأنترنت في ذلك الوقت، حيث تسببت في إيقاف الشبكة

بعض الوقت، ولما قبض عليه بعد قليل، أفاد أنه لم يكن يقصد أن يتسبب بخسائر

تتراوح بين 15 إلى 100 مليون حسب تقديرات الخبراء، وواجه الحكم عليه بأقصى

عقوبة وهي الحبس لمدة خمس سنين، وغرامة مالية قدرها 250 ألف دولار، إلا أنه

حكم عليه بثلاث سنوات فقط وغرامة مالية قدرها 10 آلاف دولارا... وفي نفس

السنة تم الفصل بين الشبكة العسكرية المحظور الاطلاع عليها milnet وبدية

الإنترنت لـ 1989 Arpanet القبض على خمسة جواسيس من ألمانيا الغربية الا بعد

أن اكتشف المخبر كليفورد ستول اختراقات منتظمة لأنظمة الحاسب في كل من

جامعة كاليفورنيا والحكومة الأمريكية، واعترفوا بعد ذلك ببيعها للاستخبارات

السوفيتية KGB، وحكم عليهم بالسجن، إلا أن أحدا منهم لم يقض أي يوم خلف

السجن؟ وفي نفس السنة تم القبض على كيفين ميتيك أحد أشهر الـ hackers

والحكم عليه بالسجن، قضى فيه سنة واحدة، ثم أطلق سراحه بعد أن أخذ عليه

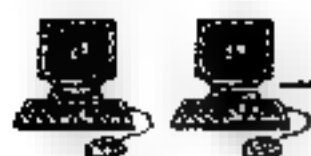
تعهد بعدم استخدام الكمبيوتر أو الاتصال بالـ 1990 hackers القبض والحكم

على ثلاثة من أربعة أشخاص سرقوا معلومات عن طريق اختراق شبكة هاتف

الطوارئ الأمريكية، كان يمكن أن تستخدم في إيقافها أو إرباكها. تراوحت

الأحكام بين 14 و 21 شهرا بالسجن.





1991 مراهقون هولنديون استطاعوا الوصول إلى أنظمة وزارة الدفاع الأمريكية إبان حرب الخليج وسرقة وتغيير معلومات حساسة عن أفراد العمليات، والمعدات العسكرية المستخدمة في الحرب وطرق تصنيعها.

1992 خمسة مراهقين من جماعة سادة الخداع اخترقوا العديد من الأنظمة ومنها بنك أمريكا، شركة AT&T، وكالة الأمن القومي.

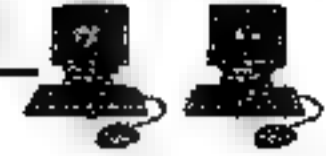
1994 جماعتان من الـ hackers اخترقتا مئات الأنظمة ومنها نظام قاعدة جريفيث الجوية، وأجهزة ناسا، ومعهد الأبحاث الذرية الكوري.

1995 القبض مرة أخرى على كيفين ميتيك بعد اعترافه باختراق العديد من الأنظمة، وسرقة حوالي 20000 بطاقة ائتمان، وظل بالسجن حتى مارس 1999 حيث قضى 10 أشهر أخرى وأطلق سراحه في يناير 2000، حيث لا يجوز له استخدام الكمبيوتر إلا بعد موافقة مكتب المراقبة التابع له. أيضا تم القبض على الروسي فلاديمير ليفين بعد القبض عليه في بريطانيا لسرقته حوالي 3.7 مليون دولار من سيتي بنك، ثم تم ترحيله إلى أمريكا حيث حكم عليه بالسجن لمدة 3 سنوات وتعويض مالي قدره 240 ألف دولار لسيتي بنك.

1997 عشرات الآلاف من المستخدمين لم يتمكنوا من الوصول إلى المواقع المراد الوصول إليها، حيث طور أوجين كشيورف، برنامجا حول وجهة هؤلاء المستخدمين إلى شركته.

1997 AlterNIC نجح أحد الهاكرز في اختراق شبكة أجهزة الكمبيوتر بوكالة الفضاء الأمريكية ناسا وقام بتحميل منظومة الاتصالات في ناسا بمعطيات معلوماتية أكثر من طاقتها، مما عرض مهمة مكوك فضاء تابعة للوكالة لخطر حقيقي، وقال رائد الفضاء <مايكل فاولا> الذي كان على متن المكوك الذي التحم مع محطة <مير> المدارية الروسية - : إن المتخصص تمكن من الدخول إلى أجهزة الكمبيوتر المسؤولة عن مراقبة دقائق قلب رواد الفضاء ونبضهم وأحوالهم لصحية العامة.





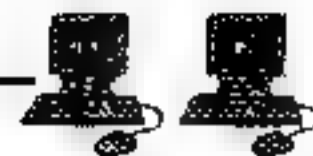
هيماء أفاد مفتش عام بوكالة ناسا - في مقابلة أجريت له ضمن برنامج <بانوراما> الوثائقي التحقيقي الذي تنتجه هيئة الإذاعة البريطانية بي بي سي - بأن درجة انتهاك هذا المتخصص لأجهزة الوكالة المتطورة جدا، وصلت إلى مرحلة أصبح معها قادرا على الدخول إلى موجات الاتصال فيها، ومعرفة معلومات عن السجلات الصحية لرواد الفضاء. وقالت الـ <بي بي سي>: إن وكالة ناسا تعرضت لهجمات عديدة من متلصصين بلغت خلال العام 1999 وحده أكثر من 500 ألف هجوم عبر الإنترنت!

1998 اختراق البنتاجون والعيب بملفات رواتب العاملين وبياناتهم الشخصية. تم القبض بعد قليل على مراقبين من وكالة فورنيا على ذمة تحقيقات الاختراق ثم بعد 3 أسابيع تم القبض على مراقب إسرائيلي يدعى <المحلل> لاتهامه بأنه العقل المدبر للاختراقات. أيضا أعلنت جماعة سادة الإنزال أنها اخترقت البنتاجون وأن لديها معلومات حساسة سوف تبينها للإرهابيين، بينما أنكرت البنتاجون هذه الادعاءات.

1999 اختراق مواقع مجلس الشيوخ الأمريكي، البيت الأبيض، الجيش الأمريكي، وعشرات المواقع الحكومية الأخرى بتوقيع <زايفلون>. 2000 إغراق مواقع عملاقة مثل ياهو، أمازون.كوم، إي باي، سي إن إن، بطريقة denial of service attack وفي أغسطس (2002)، نجح خبراء أمنيون (أو هكرز رسميون) بإحدى شركات الاتصالات الأمريكية في اختراق شبكة كمبيوتر الجيش الأمريكي، حيث كشفت الشركة النقاب عن أنها تمكنت من اختراق أجهزة حاسب تابعة للجيش، وتمكنت من الحصول على معلومات عسكرية وحكومية حساسة دون موافقة.

واستخدم خبراء أمنيون في شركة <فورنزيك تك>، برنامج محانية واسعة الانتشار خلال فترة الصيف، لتحديد أجهزة الكمبيوتر التي لا تتمتع بحماية من الاختراق، وتمكنوا من قراءة رسائل بريدية ورسائل شخصية وبيانات مالية. وقد نجح هؤلاء الخبراء في التسلل لشبكة كمبيوتر قاعدة <فورت هود> العسكرية



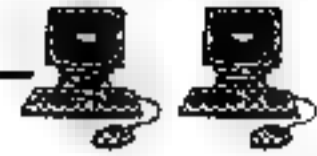


أثناء قيامهم بعمل مختلف، وتمكنوا عبر هذه الشبكة من اختراق قواعد عسكرية أخرى ومؤسسات مدنية مثل وكالة الفضاء الأمريكية <ناسا> وورارتي الطاقة والنقل الأمريكيتين، واكتشفوا أن غالبية أجهزة الكمبيوتر تستخدم فيها كلمات سر يسهل التوصل إليها مثل اسم المستخدم، أو كلمة Password ذاتها - أي كلمة السر بالإنجليزية - وتمكن المستشارون من قراءة رسائل بريد إلكتروني تبادلها ضباط كبار، والتفاصيل المالية لقطاع التجنيد، وتسجيلات لآليات فك الشفرة اللاسلكية.

وقال <بريت أوكيفي> رئيس شركة <فورنزيك تك> إن الشركة أعلنت عن تمكنها من اختراق أجهزة الكمبيوتر الخاصة بالجيش لأنها رأت أنه من الضروري لفت الأنظار للثغرات الأمنية. وأضاف: شعرنا بالصدمة وبالخوف من سهولة اختراق أجهزة الكمبيوتر، إنه مثل المرور بمبنى وزارة الدفاع ورؤية باب مفتوح دون أن يكون عليه حراسة.

واعترف الكولونيل <تيد دما توسكي> المتحدث باسم الجيش الأمريكي بتعرض شبكة الكمبيوتر الخاصة بالجيش للاختراق، لكنه قال إن المواد التي تمكنت الشركة من الحصول عليها غير سرية وإن الاختراق <لم يؤثر في الأمن القومي> وأضاف أن <الثغرات الأمنية لم تكن خطيرة، وإذا قدرناها على مقياس من عشر نقاط، فستصل درجة خطورتها لنحو 2.5 نقطة>. وإذا كان ما سبق لم يؤدي إلى حدوث ضرر على حد تعبير الكولونيل الأمريكي فبن أربعة من أنظمة الكمبيوتر الخاصة بوزارة الدفاع الأمريكية قد أصيبت - قبل ذلك بسحو عامين - بفيروس الكمبيوتر المعروف باسم فيروس الحب، وأعلنت <البيتاجون> - في بيان لها - أن الأنظمة المصابة بالفيروس قد عزلت ولم تؤثر في العمليات العسكرية، وأشار المتحدث باسم وزارة الدفاع الأمريكية إلى أن كيفية اختراق الفيروس لأنظمة الكمبيوتر بالوزارة لا تزال غامضة، رغم أن تلك الأنظمة معزولة وتتمتع بقدر عال من السرية.





وهناك من الهاكرز من يعملون بهدف السرقة والكسب المالي، ومن ذلك ما قام به أحد قراصنة الكمبيوتر حيث نجح في اختراق 5٠6 مليون حساب تابع لشركتي <فيزا كارد> و<ماستر كارد> وذلك بتجاوز أنظمة تأمين الشركتين. وذكرت شبكة CNN الإخبارية - عبر موقعها على الانترنت - أن الشركتين قامتتا هور اكتشاف عملية القرصنة بإبلاغ البنوك التي تصدر بطاقات فيزا و<ماستر كارد> وقال المتحدث رسمي باسم بنك <سيتيزن> - شمال شرق الولايات المتحدة - أنه تم إغلاق 8800 حساب لعملاء تم اختراق أرصدتهم بعد قيام شركة <ماستر كارد> بالإبلاغ عن الواقعة!

أما أغرب الاختراقات الأمنية على الانترنت، فهو ما حدث مع عملاق تكنولوجيا البرمجيات، وهكسبري شركات برامج الكمبيوتر، شركة مايكروسوفت، حيث تمكن المخترقون من الوصول إلى التصميمات الأصلية لنظم تشغيل وبرامج <ويندوز> التي تنتجها الشركة، التي يعمل بها نحو 90% من أجهزة الكمبيوتر الشخصية في العالم. وخلال هذا الهجوم، تبين أن أصول البرمج قد سرقت. وأن المتسللين ربما أتاحت لهم الفرصة للتلاعب في <الشفرة> التي كتبت بها أصول البرامج. وبينما حولت مايكروسوفت ملف الهجوم إلى مكتب التحقيقات الفيدرالي، ملتزمة الصمت تجاه الفضيحة، فقد أكدت صحيفة <وول ستريت جورنال> أن بعض الموظفين بمايكروسوفت كشفوا التسلل، عندما تعرفوا إلى بعض كلمات السر، التي أرسلت عن طريق البريد الإلكتروني إلى حساب مشترك في مدينة <بترسبورج> بروسيا، واتضح أن كلمات السر هذه قد تم استخدامها لنقل شيفرة بعض البرامج.

حروب القرصنة بين العرب والإسرائيليين

هناك هجمات متبادلة بين الهاكرز العرب والإسرائيليين حيث يسعى كل فريق لإحداث أكبر الأضرار بالطرف الآخر وقد ذكرت بعض الصحف طرفاً من تلك المعارك، فعلى سبيل المثال ذكرت صحيفة الجزيرة السعودية أن الهاكرز





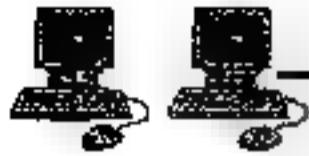
العرب نحسوا طوال الأيام الماضية فى إغلاق أكثر من 35 موقعا إسرائيليا من بينها موقع حكومية وعسكرية وتجارية مهمة بينما لم يتمكن القراصنة الإسرائيليون وحلفائهم سوى من إغلاق 12 موقعا عربياً.

حمسة منها تابعة لحزب الله اللبناني وتلفزيون المنار واثنان آخران لحركة حماس الفلسطينية واثنان تابعان للسلطة الوطنية الفلسطينية بالإضافة إلى موقع [jmi] وهي شركة إسلامية لها عدة فروع فى أستراليا وأمريكا وموقع < البوابة > الذى تعرض لهجوم محدود فى بداية الحرب، وذكر المتحدث باسم وحدة جرائم الإنترنت فى إدارة حماية البنية التحتية التابعة للوكالة NPIC

إن هذه الهجمات قد تشمل حرياً فيروسية تستهدف تدمير البنية التحتية لهذه المواقع خاصة بعد انضمام قراصنة مكويين ومجريين وبرازيليين وبلغاريين وفلبينيين محترفين إلى الطرف العربى فى هذه الحرب تعاطفاً مع الشعب الفلسطينى، بالإضافة إلى خمس جماعات قرصنة إسلامية على رأسها جماعة المهاجرين فى بريطانيا والنادي العالمى للقراصنة المسلمين MCH وجماعات جى فورس وآزاد شير وزيند أباد الباكستانية التى اشتهرت فى تاريخها الطويل مع عالم القرصنة باستهداف البنية التحتية لشبكات الكمبيوتر.

من جانبهم الإسرائيليون يطلبون وقف إطلاق النار فى معركة قصف مواقع الإنترنت المتبادلة بينهم وبين العرب والتى قدرت بعشرات الألوف من محاولات التسلل والقصف الإلكتروني من جانب المتسللين العرب لمواقع الإنترنت الإسرائيلية الرسمية، بما فى ذلك موقع مكتب رئيس الحكومة ووزارة المالية ووزارة الدفاع الإسرائيلية. وقد جرت الهجمات بواسطة إرسال آلاف الرسائل فى البريد الإلكتروني تحمل شعارات (الموت لليهود) بكثافة شديدة مما سبب انهيار الحواسيب الإسرائيلية وتعطيل عمل مكتب رئيس الوزراء لأنها أدت إلى تباطؤ عمل الحواسيب وإرسال الرسائل عبر البريد الإلكتروني.





وتبين أنه في عدة حالات جاء الهجوم من مصر والسعودية وكذلك وصل الهجوم من هواة الإنترنت في الولايات المتحدة الأميركية وأوروبا خاصة مستخدمي خدمات البريد الإلكتروني المجانية مثل (ياهو) و(هوت ميل) ..

وقد احتلت الهجمات الإلكترونية العربية حيزاً كبيراً من اهتمام الباحثين والمسؤولين الإسرائيليين وقد هدد بعضهم بالرد على الهجمات العربية الإلكترونية بينما قالت مصادر إسرائيلية إن هناك إجماعاً لدى غالبية المسؤولين الإسرائيليين بالتوصل لهدنة إلكترونية مع العرب نظراً للأضرار الفادحة التي لحقت بالحواسيب الإسرائيلية وانعكاس ذلك على أداء المؤسسات الرسمية الإسرائيلية والسمعة الدولية التجارية للحواسيب الإسرائيلية.

وقال نواف مصالحة نائب وزير الخارجية الإسرائيلي: لقد أبرمت إسرائيل مؤخراً اتفاقيات مع شركات أميركية في مجال البرمجة والحواسيب وصناعات التكنولوجيا المتقدمة بمليارات الدولارات وهي أحد الأبواب الواسعة للتجارة الإسرائيلية الجديدة وقد حذر خبراء إسرائيليون من أن استمرار عمليات (القصص الإلكتروني) العربية ستضر في نهاية الأمر بإسرائيل.

الهجوم الإسرائيلي على سوريا

في ٦ من شهر سبتمبر من عام ٢٠٠٧، كانت الحكومة السورية على موعد مع هجوم مباغت من قبل دولة الاحتلال الإسرائيلية.

الهجوم استهدف منطقة إنشاء والتي يُعتقد بناءً على الاستطلاعات الإسرائيلية - بأنها لمشروع إنشاء مركز لتصنيع أسلحة دمار شامل مشترك ما بين السلطات السورية مع كوريا الشمالية .

أُستخدمت طائرات من نوع F15 و F16 للهجوم على هذه المنطقة وتدميرها بالكامل في تلك الليلة. الفضل من جهة سلاح الدفاع الجوي السوري كانت في عدم التقاط الرادارات الروسية الصنع للطائرات الإسرائيلية عند دخولها المجال الجوي السوري تقوم عمل الرادارات على إرسال ذبذبات من موقعها إلى السماء بشكل





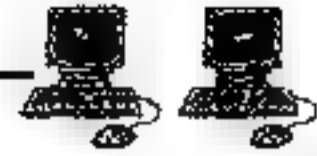
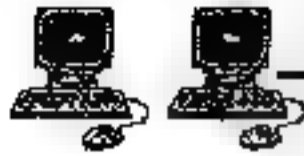
متفرق وفي حال اصطدام هذه الذبذبات بجسم معين ستعكس الموجة للرادار فيتم حساب سرعة الجسم، وارتفاعه، ومن ثم يتم تحديد شكل وتوقع الجسم في بعض الأحيان من قبل نظام الرادار .

السؤال المحير، كيف لم تلتقط الرادارات السورية تحرك طائرات كبيرة الحجم دخل مجالها الجوي، تقوم بالتفجير والتدمير وتعود لإسرائيل (عبر الحدود التركية) بدون التقاطها؟ هل الرادارات الروسية الصنع التي تم بيعها لسوريا كانت فاشلة؟ هذا لا يصدق فروسيا معروفة بقوتها في مجال الصناعات الحربية والاتصالات. هل تم تعطيل الرادارات السورية بفعل فاعل كإختراق لأنظمتها من قبل الجيش الإسرائيلي قبل البدء في الهجوم.

الأرجح حسب المحللين هو أنه بالفعل قامت إسرائيل بتخطيط محكم ودقيق قبل الهجوم وذلك بإختراق رادارات السلاح الجوي السوري وتعطيلها قبل البدء في الهجوم المباغت، يقول ريتشارد كلارك هناك ثلاثة تصورات للخلل الذي حصل للرادارات الجوية السورية:

1- بعض وسائل الإعلام قالت بأن الجيش الإسرائيلي استخدم طائرات من غير طيار تحلق في سماء سوريا، هذه الطائرات إما أن الرادارات السورية لم تلتقطها بسبب أن هذه الطائرات لها القدرة على امتصاص الذبذبات أو أنها تقوم بأخذ هذه الذبذبات وتعيد إرسالها للرادارات بطريقة معينة (كإستغلال ثغرة في هذه الأجهزة) لتصل إلى أجهزة التحكم بالرادار فتعطّلها. في هذه الحالة ماسيراه الجيش السوري هو عبارة عن سماء صافية كأي يوم عادي خالية من الأجسام الدخيلة. هذه التقنية تمتلكها حليفة إسرائيل وهي الولايات المتحدة وتسمى بـ Senior Suter

2- التصور الثاني، هو أنه تم زرع برنامج خبيث (Trojn Horse) بطريقة ما في نظام الدفاع الجوي السوري. كان البرنامج ينتظر أن يتم تفعيله من قبل الجيش الإسرائيلي إما عبر إرسال إشارة معينة من قبل طائرة متخفية قبل الهجوم ليبدأ بعمله بتعطيل نظام الرادار للجيش السوري فلا يلاحظوا وجود أي جسم غريب في



مجالهم الجوي، أو بوجود عميل إسرائيلي داخل الأراضي السورية استطاع التوصل لأماكن حساسة لزرع هذا البرنامج الضار.

3. التصور الأخير ذو احتمال ضعيف حسب ريتشارد كلارك وهو أنه تم بطريقة ما قطع أحد كوابل الألياف الضوئية السورية الخاصة بشبكة الجيش وربطها بكابل ضوئي آخر (تسمى هذه العملية Splicing) ضار من قبل عميل إسرائيلي، ومنها تم اختراق شبكة الجيش السوري والوصول لأجهزة الرادارات وتمطيلها قبل وقت الهجوم.

مهما كانت الطريقة المستخدمة من الجيش الإسرائيلي، فقد بينت مدى قوتهم في استخدام التقنية لتكتيكات حربية وكان مثال قوي و كافٍ ليرعب البقية. بالمناسبة قبل بدء غزو العراق كان الجيش الأمريكي يخطط لهجوم مماثل لإختراق نظام الرادارات للسلاح الجوي العراقي، وذلك للسيطرة التامة على المجال الجوي وتسهيل الهجوم الأمريكي بكل بساطة من قبل الطائرات الحربية. لكن هذا النوع من الهجوم لم يتم

- إيران والهجوم على المفاعل النووي

في سنة 2010 تم تسجيل أول هجوم تدميري من نوعه على المفاعل النووي "بوشهار و ناتانز" في إيران من قبل تحالف دولي بين إسرائيل وأمريكا. كان الهجوم على نظام خاص بالتحكم والمراقبة (تسمى هذه الأنظمة بـ SCADA) في عمل المفاعلات النووية في هذه المصانع.

الهجوم تم عن طريق استخدام وصلة USB تم وصلها بالنظام تحمل برنامج ضار في خطة مدروسة بعناية من قبل الدولتين المهاجمتين. انتشر الفايروس بين أجهزة التحكم بطريقة ذكية حيث يقوم بالبحث عن هدف و نوع محدد من أجهزة التحكم في عمل أجهزة تخصيب اليورانيوم، فإذا وُجد الهدف بدأ بالعمل التخريبي وإذا لم يجده فسيكمل الإنتشار والبحث عن أجهزة جديدة في الشبكة.

كان العمل التخريبي هو بتمريع عملية تخصيب اليورانيوم عن طريق التحكم في بعض الأجهزة الخاصة بذلك بطريقة غير ملحوظة للعاملين هناك بحيث





تقوم بتقديم قراءات مفلوطة على شاشات المراقبة توضح أن كل شيء يعمل على مايرام إستخدام الفيروس ثغرات غير منشورة في نظام ويندوز في ذلك الوقت، لأخذ صلاحيات أكبر والعمل كمسؤول للنظام واستغل أيضاً ثغرات في البرنامج المشغل لنظام التحكم والمراقبة المطور من قبل شركة سيميتز.

تسبب هذا الفيروس المسمى بـ **Stuxnet2** بتعطيل عملية تخصيب اليورانيوم في المفاعل وعطل تقدم البرنامج النووي الإيراني لمدة سنتين منذ زرع الفيروس في عام 2009.

عمل مثل هذا الفيروس تطلب خبراء بكفاءات عالية في عمل أنظمة التشغيل وبدراسة داخلية في كيفية عمل المصنع بأدق التفاصيل، في غالب الأمر تم استخدام عملاء بالداخل "عملاء مزدوجين".

أيضا هذا العمل التخريبي تطلب وجود مبرمجين على قدر عال من الإحتراف في عملهم.

توضح التقارير أن تكلفة إنتاج **Stuxnet** تجاوزت ملايين الدولارات. تعتبر هذه الحادثة صفة قوية لجميع الشركات المطورة لأنظمة التحكم والمراقبة في المصانع بسبب تسليط الضوء وتعريف المخربين والباحثين بضعف حماية هذه الأنظمة و لعواقب السلبية الكبيرة التي قد تلحق بالبنية التحتية لدولة في حال إستغلال هذه المشاكل في عمل تخريبي.

تجدر الإشارة هنا أنه بعد هذه الحادثة عمل كثير من الباحثين الأمنيين في البحث واكتشاف ثغرات جديدة في أنظمة التحكم والمراقبة بالإضافة لبرامج تستغل هذه الثغرات مثل **Metasploit** و **Agora SCADA+6**

مثل هذه الحوادث وغيرها من الهجمات المستهدفة من قبل دولة معادية لدولة أخرى يجب أن تكون إنذار قوي للحكومات العربية للنظر بجدية والعمل الجماعي لبناء جيش إلكتروني لكل بلد، ففي القريب العاجل ستتحوّل ساحة المعركة الى فضاء للإنترنت، وبما أننا مستهلكون للتقنية لا منتجون ستكون الضربة موجعة اذا لم يتم أخذ أمن المعلومات بجدية تامة.





عدد من الدول صرحت وبشكل واضح عن تطويرها لجيش إلكتروني مثل الصين وكوريا الشمالية للدفاع عن بلادهم والهجوم على أخرى لفرض التجسس، والتخريب وغيره.

الوضع في الدول العربية مختلف، فلا يوجد أي تحرك واضح لبناء جيوش إلكترونية تقوم بالدهاع والرد في حال وقوع أي هجوم -لا سمح الله- فأمّن المعلومات جانب تم تغييبه وعدم النظر اليه بجديّة.

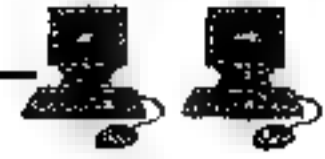
فبعض الجهات يمكن اختراقها بكل بساطة. ماذا لو كانت هذه الجهة حساسة تحتفظ بمعلومات المواطنين وتمت سرقتها الهجمات المنظمة المستهدفة لن تكون بفرض الإحراج كتغيير الصفحة الرئيسية للموقع بل ستكون لإستغلال المعلومات والتوغل أكثر في الهدف حتى تحقيق المطالب من الهجوم. كل ما ينطبق على المعارك الحقيقة من تنظيم وتكتيك ينطبق على الحروب الإلكترونية.

أساليب الحرب الإلكترونية

- 1 - القرصنة الإلكترونية،
- 2 - التسلل الإلكتروني والخداع الإلكتروني الذي يعرف بإرسال معلومات خاطئة بهدف الحصول على أخرى صحيحة ومهمة.
- 3 - التحريض الإلكتروني عبر استخدام مواقع التواصل الاجتماعي كالفيس بوك والتويتر.
- 4 - الهجوم الإلكتروني مثل استخدام المهدات الإلكترونية لشن الحرب كاستخدام طائفة من دون طيار كما ذكر سابقاً.

تعد دولة الإمارات من أكثر الدول استخداماً للإنترنت، فحوالي 3 مليون شخص فيها أي نحو 69% من سكانها يستخدمون الإنترنت في مجالات عدة ونسبة 40% من السكان يستخدمون مواقع التواصل الإلكتروني





الشيء الذي جعلها تنتشر وعياً اجتماعياً حول خطورة الحرب الإلكترونية وكيفية الحفاظ على البيانات الشخصية والمعلومات السرية لمستخدمي الانترنت على أراضيها.

وضمن الحديث عن تأثيرات الحرب الإلكترونية على دولة الإمارات، كان لا بد من الوقوف عند الخسائر المباشرة والغير مباشرة للدولة والتي حُلِفَتْها عمليات السطو والقرصنة الإلكترونية على أجهزة الكمبيوتر. فقد بلغت في العام 2011 حوالي 2.3 مليار درهم. إنها خسائر فادحة لكنها جاءت كتقدير مدروس من قبل شركات داخل الإمارات.

ومع أنها دولة مسالمة، يبدو من الطبيعي للبعض أن تتعرض دولة الإمارات لعمليات قرصنة وشن حرب إلكترونية عليها، باعتبارها تصنف كواحدة من بين أفضل خمس حكومات في العالم.

لكنها ورغم أية خسائر، تمتلك حكومة الإمارات نظام حماية قوي ضد عمليات القرصنة والهجوم الإلكتروني بكل أنواعه. إنها تتوّج وسائل دفاعها لتبقى مستعدة لأي تطوير قد يحدث عند الطرف المضاد. خاصة وأنّ علاقة غير حميمة بدولة إيران على صعيد المثال.

وكان قد تم إنشاء الهيئة العامة لتنظيم الاتصالات في الدولة في العام 2003 بمرسوم اتحادي، في شأن تنظيم الاتصالات في الدولة.

وتعتبر الهيئة الواجهة الأساسية لتصدي حملات الهجوم الإلكتروني، كما أنها تلعب دوراً هاماً في توعية الاستخدام المجتمعي لوسائل الاتصال الإلكترونية.

ولا تقتصر مهام الهيئة على حماية المنظمات والمؤسسات الحكومية في الإمارات، سواء كانت مدنية أم عسكرية. إنها تهتم أولاً بحماية الأفراد الذين من المحتمل أن يتعرضوا لسرقة أرقامهم السرية وبياناتهم الشخصية وذلك بسبب وجود فئة أفراد يتفنون بسرقة معلومات الآخرين والتجسس عليهم.





ذكرت أحدث دراسة عن القرصنة الإلكترونية أن الولايات المتحدة لا تزال هي الهدف الأول كضحية لهجمات القرصنة الإلكترونية في عام 2003، بينما احتلت البرازيل قائمة الدول التي تصدر عنها هذه الهجمات.

وقالت الدراسة التي أعدها مؤسسة «أم أي تو جي» mi2g المتخصصة بمناسبة مرور عامين على أحداث 11 سبتمبر وثلاثة أعوام على لانتفاضة الفلسطينية، أن أكبر الخسائر التي لحقت بالانترنت خلال شهر سبتمبر الماضي قد جاءت من جراء هجمات شنّها قراصنة من البرازيل (10233 هجمة صريحة) ثم من تركيا (1312 هجمة) ثم المغرب (210) وأخيرا السعودية (65 هجمة) وقالت «أم أي تو جي» أن الدافع الرئيسي لقراصنة البرازيل من وراء تلك الهجمات هو إثبات الذات واستعراض المهارات بجانب نشاط الجريمة المنظمة.

وأشارت الدراسة إلى أن الولايات المتحدة هي الهدف رقم واحد من هجمات القراصنة حيث تعرضت لنحو 71868 هجمة في الفترة من سبتمبر 2002 وحتى سبتمبر 2003 تليها ألمانيا (17529) ثم البرازيل (14785) وبريطانيا (13417) وكان تقرير أمني صادر عن مؤسسة «ميتوقز» البريطانية.

أحزاب القرصنة

إن دور هؤلاء لم يقتصر فقط على إذكاء الثورات وإنما أسهم أيضا في دخول لاعبين جدد في حلبة ومضمار السياسة من خلال أحزاب القرصنة التي بدأت في أوروبا بظهور حزب القرصنة السويدي ...امتداد لموقع خليج القرصنة للدفاع عن الحقوق الرقمية والمناهض لحقوق المؤلف : والمؤيد للقرصنة، بما في ذلك حرية الاعلام، والعاء براءات الاختراع وحقوق الطبع والنشر.

وفي عام 2009 : اصدر القضاء احكاما بالسجن وغرامات باهظة على اعضاء بحزب القرصنة جراء انتهاك حقوق التأليف والنشر، مما أدى إلى احتجاجات وتعاطف اسفرت عن نمو هائل في عضوية الحزب حيث ارتفعت بسرعة





إلى نحو 18000 عضواً، ومحققاً إنجازاً كبيراً بفوز الحزب بمقعدين في البرلمان الأوروبي بانتخابات يونيو 2009 .

و يوجد حالياً نحو 40 حزب قرصان في العالم مستوحياً المبادرة السويدية، ومن بين الدول التي يوجد بها أحزاب القراصنة كل من النمسا والدنمارك وفنلندا و ألمانيا وأيرلندا وهولندا وبولندا وإسبانيا وسويسرا..

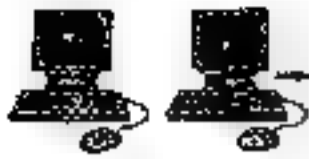
وفي أبريل 2010 تأسست رابطة القراصنة الدولية في بلجيكا ومعظم أعضاء أحزاب القراصنة من الشباب المتعلمين والمتميزين في تكنولوجيا المعلومات واستخدام الانترنت ومواقع التواصل الاجتماعي: تويتر ويوتيوب والفيسبوك ويجيدون أساليب اجتذاب الرأي العام، في المملكة المتحدة ثلاثة من أصل ثمانية مرشحين من حزب القراصنة في الانتخابات العامة في 2010 لم تكن تتجاوز أعمارهم 19 عاماً فقط وكان أكبرهم 4 عاماً .

ويصنف القراصنة في ألمانيا حزبه باعتبارهم حزب ليبرالي اجتماعي يسعى إلى تغيير جذري في أسلوب السياسة، وأعضاء الحزب قادمون من جميع أنواع الخلفيات السياسية، ويعتبرون أنفسهم في قتال من أجل الحريات الأساسية على شبكة الانترنت وضد المحاولات الحكومية الترامية إلى تقييد حرية الصحافة وحرية التعبير.

حزب القراصنة العرب

قرب المغرب العربي من الشاطئ الأوربي، وهجرة أبناء تونس والمغرب إلى أوروبا ... أدت إلى رسو سفينة القراصنة على شاطئ تونس والمغرب، وفي عام 2010، تأسس حزب القراصنة التونسي وهو أول فرع لرابطة القراصنة الدولي في قارة أفريقيا، و كسب الحزب سمعة أثناء الثورة التونسية، حيث تم اعتقال عدد من أعضاء الحزب لمشاركتهم في الاحتجاجات، وقد اختير أحد فاعلياته ليشغل منصب الكاتب العام لوزارة الشباب والرياضة في الحكومة التونسية المؤقتة. وتعتبر هذه أول مرة يحقق فيها عضو من حركة حزب القراصنة الدولي منصبا سياسيا على المستوى



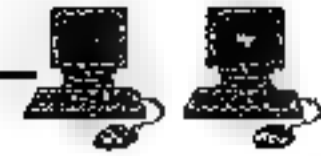


الوطني، ولكن سرعان ما قام بتقديم استقالته بعد قرار المحكمة العسكرية بغلق بعض المواقع الإلكترونية.

وفي المغرب نصح القراصنة الجدد حزبا افتراضيا بين خيوط الشبكة العنكبوتية "الإنترنت" يطالبون من خلاله بالحرية والديمقراطية، وتوفير أجواء من الحرية الحقيقية من خلال تحرير الإنترنت، ورفع كافة القيود بمختلف أصنافها القانونية والسياسية على ولوج الإنترنت والإبحار في صفحاته، زيادة على رفضه للاحتكار الذي تمارسه المنظمات الكبرى على الحقوق الفكرية.

ويرفع حزب القراصنة المغربي شعار الشفافية والديمقراطية والبلوغ الحر للمعلومات، وتجاوز الرقابة على الكلمة والصوت والصورة بالإنترنت تحديدا، ومناهضة للاحتكار الذي تمارسه المنظمات الكبرى على الحقوق الفكرية، حيث إن الشركات الكبرى غالبا ما تعتمد إلى احتكار مصادر المعرفة التي هي ملك كوني، وتوظفها لبلوغ أهداف تجارية واقتصادية، حتى إن كان مقابل ذلك هلاك الملايين، أو تركهم للفاقة والامية وينادي القراصنة بإشاعة المعرفة، ويناهض باعتبار أن المعرفة ذات طابع إنساني قبل أن تكون سلعة أو خدمة وليست أداة ابتزاز. والقراصنة الجدد أفراد وجماعات وأحزاب تيار قادم بفيض كاشف للأسرار والأغوار في عالم السياسة والصحافة والميديا... وتستثمر دول التقدم ذلك التيار في إسرائيل واحتضانها في روسيا وتجنيداً في الصين واحتفاء في الولايات المتحدة...





هوامش الفصل الثالث:

- 1 - شاكر عبد العزيز . الحروب الالكترونية الجزء الاول . الجمعية الدولية للمترجمين واللغويين العرب . 2011/01/02 انظر :
<http://www.wata.cc/forums/printthread.php?s=a434fb1b04b43d2aa7686acb7b944654&t=82289&pp=20&page=1>
- 2 - عصر الردع الالكتروني . الجزيرة نت . الجمعة 2012/10/26 م
<http://www.aljazeera.net/light/6c87b8ad-70ec-47d5-b7c4-3aa56fb899e2/7bf0ab16-7011-4e73-b8ee-b756385c8a78>
- 3 - بوابة الوفد الالكترونية الوفد - المواطن الصحفي - مقال القراصنة قادمون
http://www.alwafd.org/index.php?option=com_citizen&view=new&id=1831&Itemid=307
- 4 -
<http://arabhardware.net/articles/software/enterprise/2458-attacks-and-hackers.html>
- 5 - صيد الفوائد . <http://www.saaaid.net/Minute/298.htm>
- 6 - <http://www.airforce-technology.com/features/feature1625>
- 7 - http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- 8 - <http://www.langner.com/en/2011/11/09/two-years-later>
- 9 - <http://www.langner.com/en/2010/10/04/stuxnet-logbook->
[/oct-4-2010-1100-hours-mesz](http://www.langner.com/en/2010/10/04/stuxnet-logbook-/oct-4-2010-1100-hours-mesz)
- 10 - <http://aluigi.altervista.org/adv.htm>
- 11 - http://gleg.net/agora_scada.shtml
- 12 - <http://www.itsn.org.sa/Detail.asp?InSectionID=12&InNewsItemID=243>
- 13 - <http://news.ksu.edu.sa/node/35763>





14 <http://www.bbc.co.uk/news/technology-17623939>

15 - مفهوم الحرب الإلكترونية متفديات عراق السلام.

<http://www.iraqpf.com/showthread.php?t=244074>

16 - جمال غيطاس، حروب المعلومات. 2004م.

http://arabinfo.blogspot.com/2004/08/blog-post_17.html

17 - مقالة بعنوان حرب المعلومات على العنوان:

<http://www.alyascer.net/vb/showthread.php?t=7614>

18 - محمد بن سعود الخطيب، حرب المعلومات مصطلح عصري لمبدأ أزلي.

[http://www.sironline.org/alabwab/maqalat&mohaderat\(12\)/1202.htm](http://www.sironline.org/alabwab/maqalat&mohaderat(12)/1202.htm)

19 - مقالة بعنوان أسلحة حرب المعلومات واستخداماتها على العنوان:

<http://yomgedid.kenanaonline.com/topics/56836/posts/94428>

20 - هشام سليمان، حرب المعلومات الوجه الجديد للحروب. 2001.

http://www.islamonline.net/servlet/Satellite?c=ArticleA_C&pagename=Zone-Arabic-HealthScience/HSALayout&cid=1175947754312.

21 - مقالة عن فيروسات الحاسوب على العنوان

[/http://ar.wikipedia.org/wiki](http://ar.wikipedia.org/wiki)

22 - مقالة عن دودة الحاسوب على العنوان

<http://ar.wikipedia.org/wiki/>

23 - علي بن ضبيان الرشيد، العدوان على البيئة المعلوماتية خطورته ومواجهته.

مجلة كلية الملك خالد العسكرية العدد 81 - 01 - 06 - 2005م.

<http://www.kkmaq.gov.sa/Detail.asp?InSectionID=1689&InNewsItemID=164260>

24 - شبكة النبأ المعلوماتية - الخميس 23/حزيران/ 2011 -

20/رحب/1432.

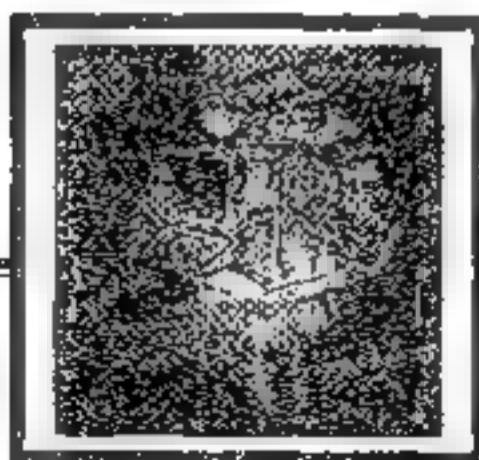


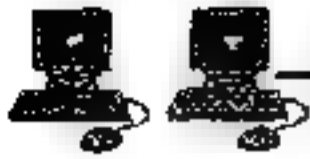


الفصل الرابع

الشبكات الاجتماعية

وانتهاك الخصوصية





الشبكات الاجتماعية (Social Network):

مصطلح يطلق على مجموعة من المواقع على شبكة الانترنت العالمية (World Wide Web)، تتيح التواصل بين الأفراد في بيئة مجتمع افتراضي، يجمعهم الاهتمام أو الانتماء لبلد أو مدرسة أو فئة معينة، في نظام عالمي لنقل المعلومات.

وجاء تعريف الشبكات الاجتماعية (social networking service) في قاموس (ODLIS): هي خدمة إلكترونية تسمح للمستخدمين بإنشاء وتنظيم ملفات شخصية لهم، كما تسمح لهم بالتواصل مع الآخرين.

ولشبكات الاجتماعية بشكل ميسر هي مجموعة من المواقع يتم من خلالها التشارك والتشبيك بين عدد من المستخدمين، يكون كل فرد منهم مجتمعه الافتراضي الخاص به الذي يقوم من خلاله بمشاركة اهتماماته وأنشطته، وكذلك تبادل الأخبار والمعلومات والملفات النصية أو المصورة، وكذلك الوسائط (مسموعة أو مرئية)، وهذه الاستخدامات غالباً ما تكون عامة وليست تخصصية في كثير من الأحيان.

ومن أشهر مواقع الشبكات الاجتماعية موقع (الفيس بوك)، الذي ظهر في فبراير من عام 2004، تلاه موقع (يوتيوب) في عام 2005، ثم موقع (تويتر) الشهير في عام 2006، وموقع (آي تون) في عام 2007، ونستطيع أن نقول: إن تسع السنوات الأولى من الألفية الثالثة قد شهدت نشاطاً كبيراً في نمو واستخدام مواقع الشبكات الاجتماعية، حيث ظهرت خلال تلك الفترة العديد من المواقع الاجتماعية.

وبسبب سرعة لعدد مستخدمي (الفيس بوك)، نجد أن عددهم في أوائل عام 2010 وصل إلى 400 مليون مستخدم، كما وصل عدد مستخدمي (تويتر) خلال المئتين نفساً إلى أكثر من 105 مليون مستخدم.

وبعد أن كان المفهوم السائد عند معظم مستخدمي المواقع الاجتماعية أن تلك الشبكات لا يتم استخدامها إلا من قبل عدد من المراهقين لقضاء أوقات التسلية، أو دون القيام بهدف محدد، إلا أن هذا المفهوم بدأ يتلاشى تدريجياً، حيث





اعتد الكثير من مُستخدمي الشبكات الاجتماعية استخدام معلوماتهم الشخصية الحقيقية؛ مثل: أسمائهم، وصُورهم الشخصية، وكذلك صُور عائلاتهم وأصدقائهم، وأحياناً كثيرة معلومات وتفاصيل عن أنشطة حياتهم اليومية.

وبالإضافة إلى ذلك فإن الشبكات الاجتماعية تتضمن محتويات معلوماتية عن الخبرات والكفاءات الشخصية، والتي يضعها المستخدمون إما من خلال نشر سيرهم الذاتية، أو حتى من خلال ملاحظة أنشطتهم واهتماماتهم على الموقع الاجتماعي، تلك المعلومات التي قد يستغلها البعض في أمور مفيدة؛ مثل: تقديم عُرُوض عمل، والاستفادة من الخبرات، وقد يتم استغلالها بطريقة سيئة قد تضر مُستخدمي تلك المواقع الاجتماعية.

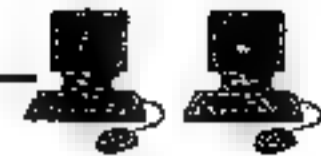
وبصفة عامة يستطيع أي شخص أن يتعرف على خصوصيات ومعلومات مهمة عن شخص آخر مستخدم للمواقع الاجتماعية؛ وذلك عبر فتح الملف الشخصي لذلك المستخدم لدقائق معدودة وقراءة ما به من معلومات.

وقد عانى موقعاً تويتر وفيسبوك على الإنترنت من مشكلات في الخوادم بسبب هجمات ثنها قراصنة مما أثار تكهنات حول حملة منسقة ضد أكثر الشبكات الاجتماعية الإلكترونية شعبية في العالم.

وتركت الهجمات التي جاءت بعد شهر من استهداف الموقع الإلكتروني للبيت الأبيض في هجوم مماثل الملايين غير قادرين على الدخول على الموقعين اللذين أصبحا بشكل مطرد جزءاً أساسياً من حياتهم اليومية.

كما ألقت الهجمات الضوء على ضعف الشبكات الاجتماعية الإلكترونية الأخذة في النمو والتي أصبحت أدوات سياسية جديدة قوية للتغلب على الرقابة والاستعداد.

وبقل تقرير في موقع سي.ان.إي.تي لأخبار التكنولوجيا عن مدير تنفيذي في فيسبوك القول أن الهجمات الإلكترونية التي وقعت كانت تستهدف مدوناً من حورجيا يشارك في الكثير من المواقع التي تأثرت بالهجمات.



وكتب ييز ستون الذي شارك في تأسيس تويتر ان الشركة تفصل عدم التكهّن بدافع الهجوم الماكر الذي تسبب في تعطل الموقع وأعاق الدخول عليه لساعات.

وأضاف ستون "يُعمل تويتر عن كثب مع الشركات والخدمات الأخرى المتأثرة بما يبدو أنه هجوم واحد منسق ضخم".

وشعر أعضاء فيسبوك أكبر شبكة اجتماعية على الإنترنت والذين يزيد عددهم عن 250 مليوناً ببطء في الدخول على صفحاتهم أو نشر مواد عليها.

ومثل تويتر قال فيسبوك انه يبدو أن المشكلات ناتجة عما يسمى بهجوم لرفض أداء الخدمة وهو أسلوب يمتطرق القراصنة من خلاله خوادم مواقع الإنترنت بطلبات اتصالات.

وبمجرد استئناف إمكانية الدخول على تويتر أرسل الكثير من مستخدمي الموقع رسائل يأسفون فيها على ما حدث.

ويبلغ عدد زوار موقع تويتر على مستوى العالم 44.5 مليون شخص في يونيو/حزيران بارتفاع قدره 15 مثلاً على أساس سنوي.

البرمجيات الخبيثة على الشبكات الاجتماعية

وفقاً لشركة ست ديفندر فإن البرمجيات الخبيثة ستزيد بنسبة 23٪ في عام 2012 إلى 90 مليون عينة، أي أكثر بحوالي 17 مليون مقارنة بنهاية عام 2011.

هذه البيانات تشكل جزءاً من تقرير بتديفسدر حول التهديدات الإلكترونية، والذي يتطلع إلى المستقبل ويتوقع تطور البرمجيات الخبيثة على الشبكات الاجتماعية مثل الفيسبوك وتويتر وحتى على أجهزة الهواتف المحمولة بالإضافة إلى نمو في الجريمة الإلكترونية.

يتوقع التقرير أيضاً أنواعاً جديدة من البرمجيات الخبيثة والاحتيال الإلكتروني التي تركز على الشبكات الاجتماعية في 2012، بينما ستزيد





البرمجيات الخبيثة المصممة خصيصاً لأنظمة أندرويد. عدد التهديدات ضد الهواتف الذكية و الأجهزة اللوحية.

”سيشهد عام 2012 نمواً هائلاً في البرمجيات الخبيثة، و يعود ذلك الى انتشار الشبكات الاجتماعية و اغراءاتها،” يقول محلل التهديدات الالكترونية في بتديفدر Bogdan Botezatu، و الذي قام بتحرير هذا التقرير. ”سيزداد عدد البرمجيات الخبيثة المخصصة لنظام أندرويد بشكل ملحوظ لكن بدءاً من قاعدة أقل بكثير من البرمجيات الخبيثة.”

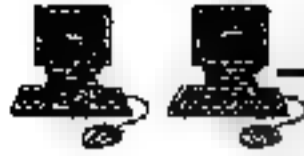
هذا التقرير هو حصيلة عام كامل من الكشف و الحماية و الازالة للبرمجيات الخبيثة حول العالم، كما انه يتضمن مراجعة لأكثر من 10 برمجيات خبيثة خطيرة في عام 2011، بالإضافة الى تغطية عن حركات الاختراق و سوء استغلال الشهادات الرقمية. و يشمل التقرير ايضاً تحليلاً للرسائل الالكترونية المزعجة و التي شكلت 75.1٪ من عدد الرسائل الالكترونية المرسلة حول العالم العام الماضي.

أنواع الشبكات الاجتماعية

تتعدد تقسيمات الشبكات تبعاً للخدمة المقدمة أو للهدف من إنشائها إلى الأنواع التالية:

- 1- تقسيم الشبكات حسب الاستخدام والاهتمام إلى ثلاثة أنواع رئيسية، هي:
شبكات شخصية لشخصيات محددة وأفراد ومجموعة أصدقاء تمكنهم من التعارف وإنشاء صداقات بينهم، مثل (Face book).
- 2- شبكات ثقافية تختص بفن معين وتجمع المهتمين بموضوع أو علم معين، مثل (Library thing).
- 3- شبكات مهنية تهتم وتجمع أصحاب المهن المتشابهة لخلق بيئة تعليمية وتدريبية فاعلة، مثل (linked in).





كما يمكن تقسيمها حسب الخدمات وطريقة التواصل إلى ثلاثة أنواع أيضاً، هي:

- 1- شبكات تتيح التواصل الكتابي.
- 2- شبكات تتيح التواصل الصوتي.
- 3- شبكات تتيح التواصل المرئي.

وتتنافس الشبكات الاجتماعية اليوم في توفير أكثر من طريقة للتواصل حتى تلبي حاجات جميع شرائح المجتمع الافتراضي.

هناك تقسيم ثالث، يقسم الشبكات الاجتماعية إلى قسمين:

1- شبكات داخلية خاصة (Internal Social Networking):

تتكون هذه الشبكات من مجموعة من الناس تمثل مجتمعا مغلوقاً أو خاصاً يمثل الأفراد داخل شركة أو تجمع ما أو داخل مؤسسة تعليمية أو منظمة ويتحكم في دعوة هؤلاء الأشخاص فقط وليس غيرهم من الناس للدخول للموقع والمشاركة في أنشطته من تدوين وتبادل آراء وملفات وحضور اجتماعات والدخول في مناقشات مباشرة وغيرها من الأنشطة، مثل شبكة (linked in).

2- شبكات خارجية عامة (External Social Networking):

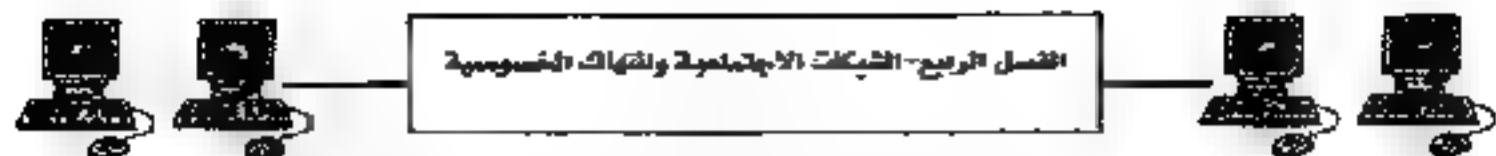
وهي شبكات متاحة لجميع مستخدمي الانترنت، بل صممت خصيصاً لجذب المستخدمين للشبكة ويسمح فيها للعديد من المستخدمين بالمشاركة في أنشطته بمجرد أن يقوم المستخدم بالتسجيل في الموقع وتقديم نفسه للموقع، مثل شبكة (Facebook).

مميزات الشبكات الاجتماعية

تتميز الشبكات الاجتماعية بعدة مميزات منها، ما يلي:

- 1- العالمية: حيث تلغى الحواجز الجغرافية والمكانية، وتتخطى فيها الحدود الدولية، حيث يستطيع الفرد في الشرق التواصل مع الفرد في الغرب، في بساطة وسهولة.





- 2- التفاعلية، فالفرد فيها كما أنه مستقبل وقارئ، فهو مرسل وكاتب ومشارك، فهي تلغي السلبية المقيتة في الإعلام القديم - التماز والصحف الورقية. وتعطي حيزاً للمشاركة الفاعلة من المشاهد والقارئ.
- 3- التنوع وتعدد الاستعمالات، يستخدمها الطالب للتعلم، والعالم لبحث علمه وتعليم الناس، والكاتب للتواصل مع القراء... وهكذا.
- 4- سهولة الاستخدام، فالشبكات الاجتماعية تستخدم بالإضافة للحروف وبساطة اللغة، تستخدم الرموز والصور التي تسهل للمستخدم التفاعل.
- 5- التوفير والاقتصادية، اقتصادية في الجهد والوقت والمال، في ظل مجانية الاشتراك والتسجيل، فالفرد البسيط يستطيع امتلاك حيز على الشبكة للتواصل الاجتماعي، وليست ذلك حكراً على أصحاب الأموال، أو حكراً على جماعة دون أخرى.

نماذج من الشبكات الاجتماعية

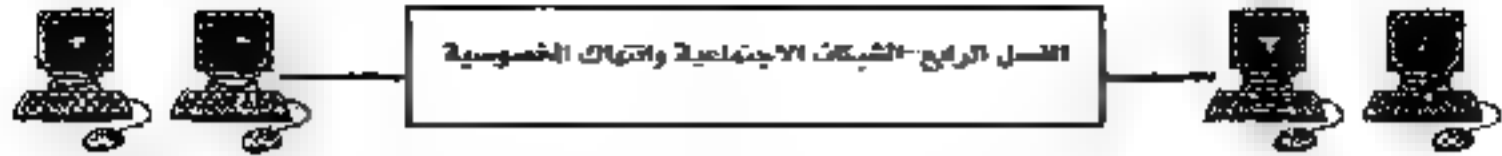
يكون الكلام في هذا البحث على نموذج من الشبكات الاجتماعية الموجودة على الشبكة، ولا يدل هذا الاختيار على الأفضلية بقدر ما يشير إلى سعة الانتشار والتداول، وخاصة على المستوى العربي، ومن بين تلك الشبكات ما يلي:

الفيس بوك (Face book):

وهو موقع يساعد على تكوين علاقات بين المستخدمين، يمكنهم من تبادل المعلومات، والملفات والصور الشخصية ومقاطع الفيديو والتعليقات. كل هذا يتم في عالم افتراضي، يقطع حاجز الزمن والمكان.

بعد موقع الفيس بوك واحداً من أشهر المواقع على الشبكة العالمية، ورائد التواصل الاجتماعي. وأصبح موقع الفيس بوك اليوم متبر افتراضي للتعبير، واتخذته الشباب اليوم بديلاً للأحزاب السياسية العاجزة القاشلة.

بدأت الفيس بوك على يد أحد طلاب جامعة هارفارد، يدعى مارك حوكر بيرج، حيث بدأ بتصميم موقع على الشبكة الإلكترونية يهدف من خلاله للتواصل مع زملائه في الجامعة، ويمكنهم من تبادل ملفاتهم وصورهم وآراءهم وأفكارهم.



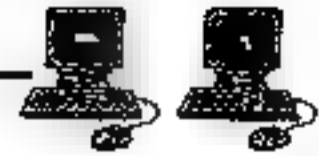
تويتر (Twitter):

هو موقع شبكات اجتماعية يقدم خدمة تدوين مصغر والتي تسمح لمستخدميه بإرسال تحديثات Tweets عن حالتهم بحد أقصى 140 حرف للرسالة الواحدة. وذلك مباشرة عن طريق موقع تويتر أو عن طريق إرسال رسالة نصية قصيرة SMS أو برامج المحادثة الفورية أو التطبيقات التي يقدمها المطورون مثل الفيس بوك و (twitterfox) وتظهر تلك التحديثات في صفحة المستخدم ويمكن للأصدقاء قراءتها مباشرة من صفحاتهم الرئيسية أو زيارة ملف المستخدم الشخصي، وكذلك يمكن استقبال الردود والتحديثات.

المدونات (Weblogs):

ظهرت المدونات في عام 1997 على يد John Barger، إلا أن انتشارها على نطاق واسع لم يبدأ إلا بعد عام 1999، وهو موقع شخصي على شبكة الإنترنت يدون فيه آراءه ومواقفه حول مسائل متنوعة، وتكون هذه المدونات مؤرخة ومرتبة زمنياً تصاعدياً. وهذه المدونات منظمة تنظيمياً ذاتياً تساعد الأفراد على التفاعل من خلال المشاركة والتعلم عبر تبادل الأفكار والمعلومات فضلاً عن حل المشكلات الاجتماعية والسياسية، ومن مميزات المدونات:

- سهولة الإنشاء، فلا تحتاج لكبير معرفة أو خبرة بلغات البرمجة، فهناك الكثير من القوالب الجاهزة المساعدة في الإنشاء والتصميم.
- سهولة التدوين والنشر، والخروج عن الأنظمة التعقيدية التحجيرية، والحجر على الأفكار والآراء.
- كسر حاجز الوقت والمكان، فيمكن للمدون التدوين في أي وقت شاء من ليل أو نهار، ومن أي مكان كان فيه، كل ما يحتاجه جهاز وشبكة وفكر فقط.
- حفظ حقوق النشر والطباعة للأفكار والكتابات والتدوينات والإخراجات
- إمكانية التفاعل مع الجمهور، وهو ما يسمى بالتغذية الراجعة (Feedback)، فيمكن للجمهور الرد والمشاركة على الموضوع المدون.



■ توفير في الوقت والجهد في التدوين والطباعة والتوزيع، وفيه حمض للبيئة من محلفات المطابع.

■ أرشفة آلية للكتابات والتدوينات زمنياً تصاعدياً، يمكن الرجوع لها سواء من لكاتب أو القارئ متى شاء.

■ إمكانية استخدام الصوتيات والفيديوهات (المتيميديا) في التدوين.

■ مساحة حرة للتطوير البرمجي، واختيار الشكل العام (الستايل) للمدونة.

الاستخدامات السلبية للشبكات الاجتماعية

إن جرائم الانترنت أخطر ما يواجه المستخدم البسيط وحتى المحترف، وإن كان العلم ولحذر قد يخفف من وطأة الجرائم، وكان حذيفة بن اليمان رضي الله عنه يسأل عن شر ليتجنبه، وليحذر منه، فكان يقول: (كان الناس يسألون رسول الله صلى الله عليه وسلم عن الخير وكنت أسأله عن الشر مخافة أن يدركني)، ومن تلك الاستخدامات السلبية ما يلي:

1- بث الأفكار الهدامة والدعوات المنحرفة

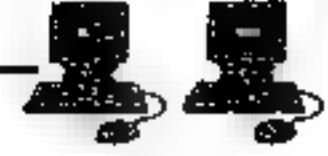
وهذا البث مما يحدث خللاً أمنياً وفكرياً، وخاصة أن أكثر رواد الشبكات الاجتماعية من الشباب مما يسهل إغرائهم وإغوائهم بدعوات لا تحمل من الإصلاح شيئاً بل هي للهدم والتدمير، وقد يكون وراء ذلك منظمات وتجمعات، بل ودول لها أهداف تخريبية

2- عرض المواد الإباحية والفاحشة

إن مسألة الإباحية الخلقية والدعارة من المخاطر العظيمة على المجتمعات القديمة والمعاصرة وقد أوردنا سابقاً قول الرسول الله صلى الله عليه وسلم: (ما تركت بعدي فتنة هي أخطر على الرجال من النساء).

لقد ذكرت وزارة العدل الأمريكية في دراسة لها أن تجارة الدعارة والإباحية الخلقية تجارة رائجة جداً يبلغ رأس مالها ثمانية مليار دولاراً ولها أواصر وثيقة تربطها بالحرمة المنظمة. وتجارة الدعارة هذه تشمل وسائل عديدة كالكاتب والمجلات





وأشرطة الفيديو والقنوات الفضائية الإباحية والإنترنت. وتفيد الإحصاءات الاستخبارات الأمريكية (FBI) أن تجارة الدعارة هي ثالث أكبر مصدر دخل للجريمة المنظمة بعد المخدرات والقمار. جرائم الإنترنت مصطلح يقصد بها (أي عمل غير قانوني يستخدم فيه الإنترنت كأداة أو محل للجريمة).

3- التشهير والمضايقة

وهي أخلاقية تظهر على الشبكة العنكبوتية بشكل عام لسهولة التدوين والتخفي على الشبكة، وهي أخلاقيات لا تحتاج بالضرورة إلى معرفة تامة بالبرمجة والبرمجيات، ولا تستند في الغالب العام إلى مستند شرعي حقيقي، فلا يحتاج صاحبها للتدليل أو التعليل أو الإثبات، كل هذا تقابله أنظمة وقوانين لا تملك الرد الرادع لمثل هذه التصرفات.

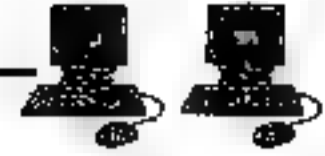
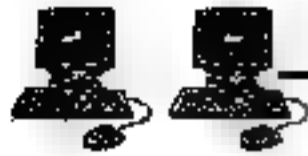
والابتزاز قد يكون أخلاقياً بصور أو مقاطع فيديو خاصة إن أخذت كرهاً وغصباً وهي من أكثر صور الابتزاز على الشبكات الاجتماعية، وقد يكون مالياً من قبل أشخاص أو من قبل عاملين في مؤسسة أو شركة خاصة عند ترك العمل أو الفصل، فقد تكون بحوزته معلومات هيساوم صاحب المؤسسة أو الشركة على تلك المعلومات.

والتزوير من أكثر جرائم نظم المعلومات انتشاراً على الإطلاق، ويتم التزوير في صور شتى منها على سبيل المثال: إدخال بيانات خاطئة أو التعديل البيانات الموجودة، ومن صورها على الشبكات الاجتماعية تزوير البيانات الخاصة للشخص مثل الجنس أو العمر أو وضع صورة مخالفة للواقع.

4- انتهاك الحقوق الخاصة والعامه

الخصوصية الشخصية الخاصة أو الخصوصية الاعتبارية للمواقع من الحقوق المحفوظة والتي يعتبر الاعتداء عليها جرمًا يستحق صاحبها العقاب والتجريم، وقد أدى انتشار الشبكة وخاصة الاجتماعية - بما تحمله من خصوصية





اجتماعية للشخص والمواقع - إلى سهولة هتك ستار الحقوق والتلاعب بها إما بالتعطيل أو التغيير أو بالاستغلال السلبي لها ولعلوماتها.

وإنتهاك الخصوصية يتم ذلك من عدة طرق، منها انتحال الشخصية الخاصة للأفراد أو الاعتبارية للمواقع والشركات، فكل شخصية فردية واعتبارية حقوقها المحفوظة. وخاصة للشخصيات المهمة والمتميزة وأصحاب الرئاسات الكبرى، وكذلك الحال مع المواقع الشهيرة والمتميزة، استغلالاً للنفوذ والشهرة والثقة الاعتبارية لكثير من الشخصيات والمواقع.

وعلى الرغم من كل الجهود المبذولة لمواجهة الجريمة المعلوماتية . إلا انه كانت هناك بعض الآثار السلبية لاستخدام شبكة الانترنت اثرت تائيرا مباشرا هي السلوكيات والتعاملات بين الافراد وبعضهم البعض نذكر منها على سبيل المثال:-

1. الأضرار الأخلاقية: والتي تعد من أبرز السلبيات التي أفرزها دخول الإنترنت إلى واقعنا حيث انتشرت ظواهر ارتياد المواقع المروجة للجنس من قبل الشباب فالشركات والمراكز المتخصصة التي تنتج وتروج الافلام الاباحية بفرض الكسب المادي، تتيح الاستخدامات اللاأخلاقية في الاطلاع على تلك الافلام الاباحية من على شبكة الانترنت وتروج لها مع ماتحملة من شذوذ وخروج عن القيم الدينية والاعراف الاخلاقية

2. الأضرار العقائدية :- والمتمثلة في المواقع التي تروج للأفكار المتطرفة واشاعة المذاهب الهدامة كالعلمانية والشيوعية والوحدوية وغيرها، وكذا المواقع التي تدعو الى الفتن الدينية ومقارنات الاديان والتي يشرف عليها اناس غير متخصصين او مؤهلين علميا او دينيا، كل هذا له خطر كبير لان تلك المواقع يكون لها الاثر في تشكيل العقول خاصة في مرحلة الشباب لما تمثله تلك المرحلة من فضول وعدم استقرار فكري وقسمي والاضرب على اوتار العقيدة وجرف عقول هؤلاء الشباب الى تيارات مناهضة الاديان او التطرف او حتى الالحاد.





3. الاضرار النفسية :- والمتمثلة فى المواقع التى تقدم برامج تتسم بالجاذبية واستخدام المنطق فى عرض افكارها، تقود الشباب من حيث لا يدري الى العنف والجريمة والتطرف والادمان لان هذه المواقع يكون لها من الاهداف الخفية التى تسعى استثارة الغرائز

4. الاضرار الاجتماعية: حيث استخدم الانترنت فى التشهير والمصايقة للآخرين حيث استخدمت البرامج التى لها شعبية وجماعية كبيرة على شبكة الانترنت فى التشهير بشخصيات اجتماعية او سياسية او حتى شخصيات عادية فى حالة اى اختلاف فى الراى او العلاقات الاجتماعية يقوم احد الاشخاص بالتشهير بالآخر عبر شبكة الانترنت وفى تلك المواقع التى يرتادها ملايين الاشخاص وهذه الظاهرة اصبحت متفشية واذا نظرنا الى المنتديات والمدونات والمواقع العربية نجد كمأ هائلاً من الاساءات الشخصية التى توجه لتلك الشخصيات حيث تعدت تلك الظاهرة مفهوم النقد لانه من المعروف ان النقد شئ والتجريح والتشهير شئ آخر.

5. ومن امثلة الاضرار الاجتماعية :- ايضا ظاهرة تكوين صداقات عبر الانترنت والتى اصبحت منتشرة بصورة مذهلة من خلال مواقع المحادثات ومواقع التعارف امثال موقع الفيس بوك الشهير حيث يقوم الشباب بوضع صورهم وبياناتهم الشخصية على تلك المواقع والتى يمكن من خلال التقنيات الحديثة استغلالها اسوأ استغلال سواء فى التشهير بصاحب تلك الصور - كما اشرنا سابقا - او فى الاستيلاء عليها واجراء تعديلات بها ووضعها على مواقع اباحية الامر الذى يستيجل معه لصاحب هذه الصور ان يقوم بحذفها او محوها لانها تكون قد استخدمت فى اكثر من موقع بمجرد تحميلها على موقع واحد من تلك المواقع

كافه هذه الاستخدامات كان لها اثارها السلبية على تربية الشباب وصرفهم عن قيم دينهم وانحراف اخلاقهم فهى تأخذ حيزاً كبيراً من الوقت الامر





لذى ادى الى عزلتهم اجتماعيا وابعدهم عن الانشطة الرياضية الاخرى التى يمكن ان يقوم بها فضلا عن ايمان بعضهم لشبكة الانترنت

المخاطر الأمنية في الشبكات الاجتماعية

وتقسم الى نوعين مخاطر عامة ومخاطر خاصة :-

أ - المخاطر العامة وتشمل :-

اولاً: الاصطياد الالكتروني

" الحصول على المعلومات الخاصة بمستخدمي الانترنت سواء اكانت معلومات شخصية او مالية عن طريق الرسائل الالكترونية او مواقع الانترنت التي تبدو وكأنها مبعوثة من شركات موثوقة أو مؤسسات مالية وحكومية "

ثانياً: انتحال الشخصية

" يقوم المهاجم بانتحال شخصية المستخدم وتزييفه ، والتظاهر على انه شخص او مستخدم ما " فيقوم المهاجم بوضع اسم مستخدم باسمك ويضع الصورة الشخصية الخاصة بك ، وقد يتكلم على لسانك وينشر اشياء غير لائقة ويتكلم بكلام بذيء.

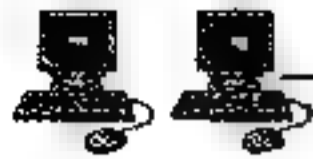
ثالثاً: الإغراق

وهو بريد الكتروني غير مرغوب فيه، يتعرض خلاله كثير من مستخدمي الشبكات الاجتماعية الى مشكلة الإغراق، فكلما قام احدكم بالتعليق على احدى الصور الخاصة بك وغيرها من الأنشطة، تأتيك رسالة على بريدك الالكتروني مما يؤدي الى امتلاء الصندوق الوارد الخاص بك بشكل سريع جداً ، مما يؤدي بعض الاحيان الى عدم استجابة بريدك الالكتروني او مسح رسائل مهمة لديك.

رابعاً: سرقة المعلومات وتعديلها :-

وتتم في الغالب عن طريق الاشخاص الذين طوروا التطبيقات على الشبكة الاجتماعية فاستخدام التطبيقات يسمح بتطويرها بالاطلاع والتطوير والتعديل على المعلومات الشخصية للمستخدمين .





ب - مخاطر عامة وهي تهدد مستخدمي مواقع التواصل الاجتماعي وتشمل:

1 - البرامج الضارة : - في عام 2011 أصبحت الوسائط الاجتماعية الوسيط

المفضل للاتصالات بالنسبة للمستخدمين الذين يقضون نحو 700 مليار دقيقة في الشهر على مواقع الفيس بوك فقط مما يجعل مواقع الشبكات الاجتماعية ومستخدميها أهدافاً مثالية للبرامج الضارة والأكواد الخبيثة

2 - فقد المعلومات: - الشبكات الاجتماعية في جوهرها قائمة على إنشاء الروابط وتكوين العلاقات ومشاركة التجارب والخبرات والمعلومات . وفي بعض الحالات ليس من المفروض ان تتاح هذه المعلومات للجمهور . ويحدث كثيراً ان ينشر الناس بشكل غير مقصود معلومات سرية على طريقة " قابلت فلان واعتقد انه سيحصل على عمولة ضخمة " أو " اشد شعري واذا لم نحصل على هذا الخلل في البرنامج بسرعة , فربما لا احصل على قسط من النوم ابدا ليلة " , وهي تصريحات تقدر معلومات داخلية عن الشركات والمؤسسات .

3 - استهلاك سعة البيانات: - صرح 40 في المائة من الموظفين انهم يستخدمون مواقع الشبكات الاجتماعية اثناء العمل , مشكلين ضغطاً وارهاقا على سعة البيانات الى الحد الذي يضر بتطبيقات الاعمال الاخرى. في العام الماضي عندما ألزمت الحكومة الالكترونية الشبكات بآتاحة الوصول المفتوح للشبكات الاجتماعية , زادت حركة البيانات في الشبكات بنسبة 25٪ في المائة فمقاطع الفيديو وحدها قادرة على اغراق العديد من الشبكات في مسار الفيديو الواحد يستهلك عادة ما بين 500 كيلو بايت الى 1,2 ميغابت في الثانية. ولانه لديك عشرات بل مئات الافراد الذين يستخدمون مقاطع الفيديو ومن السهل ادراك تأثير ذلك في تدهور الاداء العام للشبكة .

4 - فقد الانتاجية: - أصبحت مواقع الشبكات الاجتماعية وجهات مقصودة في حد ذاتها على الانترنت . اذ تمكنت من نشر الرسائل وقرائنها والبحث عن الاصدقاء والتسويق وتحميل مقاطع الفيديو وممارسة الالعاب . وهذا





يجعلها ملائمة بصورة جذابة للمستخدمين لما يحددهم لقضاء المزيد والمزيد من الوقت في هذه المواقع . ولكنها بالقدر نفسه تشكل تحديات أمام قطاع الشركات والأعمال يستلزم منها فرض القدرة المناسبة من التحكم والسيطرة . فإذا تركت بدون قيود فقد يؤثر الوقت الذين يستغرقه على الانتاجية لأن الموظفين سيقضون المزيد والمزيد من الوقت في الشبكات الاجتماعية خلال ساعات العمل .

في عصر المعلومات وبفعل وجود تقنيات عالية التقدم فإن حدود الدولة مستباحة بأقمار التجسس والبث الفضائي "و العالم العربي والإسلامي كان ولا يزال مستهدفاً أمياً وثقافياً وفكرياً وعقدياً لأسباب لا تحصى على أحد.

وقد تحولت وسائل التجسس من الطرق التقليدية إلى الطرق الإلكترونية خاصة مع استخدام الإنترنت وأن تشاره عربياً وعالمياً.

ولا تكمن الخطورة في استخدام الإنترنت ولكن في ضعف الوسائل الأمنية المستخدمة في حماية الشبكات الخاصة بالمنظمات والهيئات الحكومية ولا يمكن حتماً الاعتماد على وسائل الحماية التي تنتجها الشركات الأجنبية فهي ليست في مأمن ولا يمكن الاطمئنان لها تماماً.

ولا يقتصر الخطر على محاولة اختراق الشبكات والمواقع على العابثين من مخترقي الأنظمة أو ما يعرفون اصطلاحاً (hackers) فمخاطر هؤلاء محدودة وتقتصر غالباً على العبث أو اتلاف المحتويات والتي يمكن التغلب عليها باستعادة نسخة أخرى مخزنة في موقع آمن، أما الخطر الحقيقي فيكمن في عمليات التجسس التي تقوم بها الأجهزة الاستخباراتية للحصول على أسرار ومعلومات لدولة ومن ثم إفشائها لدول أخرى تكون عادة معادية، أو استغلالها بما يضر بالمصلحة الوطنية لتلك الدولة.

وقد وجدت بعض حالات التجسس الدولي ومنها ما اكتشف أخيراً عن مفتاح وكالة الأمن القومي الأمريكية (NSA) والتي قامت بزراعته في نظام التشغيل الشهير ويندوز، وربما يكون هذا هو أحد الأسباب الرئيسية التي دعت





الحكومة الألمانية باعلانها في الاونة الاخيرة عن استبدالها لنظام التشغيل وندوز
بأنظمة اخرى

كما كشف اخيرا النقيب عن شبكة دولية ضخمة للتحسس الالكتروني
تعمل تحت اشراف وكالة الامن القومية الامريكية بالتعاون مع اجهزة الاستخبارات
والتحسس في كندا، بريطانيا، امسترااليا ونيوزيلندا ويطلق عليها اسم
(ECHELON) لرصد المكالمات الهاتفية والرسائل بكافة انواعها سواء ماكان
منها برقيا، تلكسيا، فاكسيا أو الكترونيا.

وخصص هذا النظام للتعامل مع الاهداف غير العسكرية وبطريقة تجعله
يعترض كميات هائلة جدا من الاتصالات والرسائل الالكترونية عشوائيا باستخدام
خاصية الكلمة المفتاح بواسطة الحاسبات المتعددة والتي تم انشاء العديد من
المحطات السرية حول العالم للمساهمة في مراقبة شبكات الاتصالات الدولية ومنها
محطة رصد الاقمار الصناعية الواقعة في منطقة واي هويبي بجنوب نيوزيلندا،
ومحطة جير الدتون الموجودة باستراليا، والمحطة الموجودة في منطقة موروينستو في
مقاطعة كورنوال ببريطانيا، والمحطة الواقعة في الولايات المتحدة الامريكية
بمنطقة شوجرجروف وتبعد (250) كيلومترا جنوب واشنطن دي سي، وايضا المحطة
الموجودة بولاية واشنطن على بعد (200) كيلومتر جنوب غرب مدينة سياتل. ولا
يقتصر الرصد على المحطات الموجهة إلى الاقمار الصناعية والشبكات الدولية
الخاصة بالاتصالات الدولية، بل يشمل رصد الاتصالات التي تجرى عبر أنظمة
الاتصالات الأرضية وكذا الشبكات الإلكترونية. أي انه يرصد جميع الاتصالات
التي تتم بأي وسيلة.

ويعتبر الافراد والمنظمات والحكومات الذين لا يستخدمون أنظمة الشفرة
التأمينية أو أنظمة كودية لحماية شبكاتهم وأجهزتهم، اهدافا سهلة لشبكة
التجسس هذه، وإن كان هذا لا يعنى بالضرورة ان الاهداف الاخرى التي تستخدم
أنظمة الشفرة في مأمن تام من الغزوات الاستخباراتية لهذه الشبكة ومثيلاتها.





ولا يقتصر التجسس على المعلومات العسكرية أو السياسية بل تعداه إلى المعلومات التجارية والاقتصادية بل وحتى الثقافية .

فمع توسع التجارة الإلكترونية عبر شبكة الإنترنت تحولت الكثير من مصادر المعلومات إلى أهداف للتجسس التجاري ففي تقرير صدر عن وزارة التجارة والصناعة البريطانية أشار إلى زيادة نسبة التجسس على الشركات من (36%) عام (1994م) إلى (45%) عام (1999م).

كما أظهر استفتاء أجرى عام (1996م) لمسؤولي الأمن الصناعي في الشركات الأمريكية حصول الكثير من الدول وبشكل غير مشروع على معلومات سرية لانشطة تجارية وصناعية في الولايات المتحدة الأمريكية.

ومن الأساليب الحديثة للتجسس الإلكتروني أسلوب إخفاء المعلومات داخل المعلومات وهو أسلوب شائع وإن كان ليس بالأمر السهل، ويتلخص هذا الأسلوب في لجوء المجرم إلى إخفاء المعلومة الحساسة المستهدفة بداخل معلومات أخرى عادية داخل الحاسب الآلي ومن ثم يجد وسيلة ما لتفريب تلك المعلومة العادية في مظهرها وبذلك لا يشك أحد في أن هناك معلومات حساسة يتم تهريبها حتى ولو تم ضبط الشخص متلبساً، كما قد يلجأ إلى وسائل غير تقليدية للحصول على المعلومات السرية.

وبعد الاعتداءات الأخيرة على الولايات المتحدة الأمريكية صدرت تعليمات جديدة لأقمار التجسس الاصطناعية الأمريكية بالتركيز على أفغانستان والبحث عن أسامة بن لادن والجماعات التابعة له، وقررت السلطات الأمريكية الاستعانة في عمليات التجسس على أفغانستان بقمرين اصطناعيين عسكريين مصممان خصيصاً لالتقاط الاتصالات التي تجرى عبر أجهزة اللاسلكي والهواتف المحمولة، بالإضافة لقمرين اصطناعيين آخرين يلتقطان صوراً فائقة الدقة وفي نفس الوقت طلب الجيش الأمريكي من شركتين تجاريتين الاستعانة بقمرين تابعين لهما لرصد الاتصالات ومن ثم تحول بعد ذلك إلى الولايات المتحدة حيث تدخل في أجهزة كمبيوتر متطورة لتحليلها.





وتشارك في تلك العمليات شبكة إشبيلون المستخدمة في التجسس على المكالمات الهاتفية ورسائل الفاكس والبريد الإلكتروني، الأمر الذي يتيح تحليل الإشارات التي تلتقطها الأقمار الصناعية حتى إن كانت واهنة أو مشفرة .

مخاطر الخصوصية في الشبكات الاجتماعية

تكمن مخاطر الخصوصية في الشبكات الاجتماعية بـ :-

1 - البرمجيات الضارة

تعد الفيروسات الإلكترونية في الشبكات الاجتماعية من أنواع الديدان الكمبيوترية. و من أشهرها دودة "كوبفايس" (Koobface) و التي أنشأت أكبر عدد من الكمبيوترات المسحرة لأغراض خبيثة في بيئة الجيل الثاني من الويب وفيروس "كوب فيس" وهو عبارة عن دودة إلكترونية تنتشر عبر حسابات المستخدمين المسجلين في مواقع الشبكات الاجتماعية ذائعة الصيت من أمثال "فيس بوك" و"ماي سبيس" وغيرها، وهي تخترق قوائم الأسماء في حسابات المستخدمين وترسل لهم أخباراً وتعليقات تتضمن رابطاً لإحدى الصفحات غير الحقيقية لموقع "يوتيوب" وتطلب منهم تحميل نسخة حديثة من مشغل الوسائط المتعددة "فلاش" كي يتمكنوا من تشغيل مقطع الفيديو الموجود على موقع "اليوتيوب". وبدلاً من تحميل البرنامج يتم تحميل دودة "كوب فيس" على جهاز الكمبيوتر الخاص بالمستخدم وتتخذ منه قاعدة جديدة تشن منها غارات على أجهزة الكمبيوتر الأخرى الخاصة بالأصدقاء المدرجين في قائمة الأسماء لدى المستخدم الذي أصابت جهازه هذه الدودة.

2 - رسائل القرصنة والتصيد

و تندرج تحتها الرسائل الإلكترونية الموجهة لمستخدمي الشبكات الاجتماعية و التي تعطي رابطاً يتوجه بالضحية لموقع مزيف. مثل رسالة (FBAction) على " فيس بوك". التي تدعي إنها من مكتب التحقيقات الجنائية (إف بي آي) في أميركا. وكانت النتيجة الاستيلاء على العديد من حسابات المستخدمين. وعلى الرغم من أن هذا المصطو لم يصب سوى جزء ضئيل من





المشتركون، فإنه شكل عددا كبيرا إذا أخذنا في الاعتبار أن "فيس بوك" يضم أكثر من 350 مليون مشترك، ولكن لحسن الحظ، كان رد فعل "فيس بوك" سريعا، بحيث حول اسم الموقع وصفته، إلى اللائحة السوداء. لكن كان لهذا الأمر تداعياته، إذ تبعت ذلك محاولات مماثلة حاولت تقليد الأمر.

3 - أحصنة طروادة

عبارة عن شفرة صغيرة يتم تحميلها لبرنامج رئيسي من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية، غالبا ما تتركز على إضعاف قوى الدفاع لدى الضحية أو تقويضها ليسهل اختراق جهازه وسرقة بياناته. وتعتبر من البرمجيات الضارة الشعبية إلا أن الشبكات الاجتماعية أمدته بروح جديدة. إذ أصبح أداة للاحتيال وسرقة الحسابات البنكية و الملفات الحساسة عبر الشبكات الاجتماعية نتيجة لمعرفة المخرب لهوية الضحية وسهولة استهدافه.

4 - تسرب البيانات الشخصية والمعلومات السرية

نتيجة لشعور مستخدمي الشبكات الاجتماعية بالألفة والثقة مع من يتشاركون معهم فإنهم قد يتشاركون بأكثر مما يجب سواء في الأمور الشخصية أو متعلق بأماكن عملهم، و ما يخص شؤونهم المالية والتغييرات الحاصلة في مؤسساتهم و فضائهم. مما يتسبب في مشاكل كثيرة بدءاً من الاحراجات الاجتماعية و إنتهاء بالملاحقات القانونية. فبمجرد أن تكتب في حائطك على "فيس بوك" أنك سوف تقضي أسبوع إجازتك في تركيا، هانت حتماً بلا وعي منك تعرض منزلك للسرقة.

5 - الروابط الإلكترونية المختصرة

و أكثر ما نجد هذه المشكلة في المواقع الاجتماعية التي لا تسمح بتعدي حد معين من الكلمات كـ "تويتر" مثلاً. إذا يضطر الأشخاص لاستخدام الخدمات المختصرة لعناوين الموقع الإترنتي مثل (tinyurl) بغية حشر العناوين الطويلة في مساحات ضيقة. وهم يقومون أيضا هنا بعمل جيد لطمس وتضليل الرابط بحيث لا يبدو من الوهلة الأولى واضحا للضحايا بأنهم ينقرون فعلا على برنامج تحريري جرى





تركيبه، وليس على فيديو من قناة الجزيرة مثلاً. ومثل هذه الروابط لمختصرة سهلة الاستخدام ومتوافرة في كل مكان. ويقوم العديد من زبائن "تويتر" أوتوماتيكياً بتقصير أي رابط، مع قيام الجميع برؤية ذلك.

6 - انتحال الشخصيات

لقد جرى تخريب حسابات العديد من الشخصيات البارزة والمرموقة. دوي المكانة الدينية أو السياسية على حد سواء والذين لهم آلاف من الأتباع على الشبكات الاجتماعية. كما قام آلاف من منتحلي الشخصيات الشهيرة بجمع مئات بل آلاف من الأتباع على "تويتر" إلحاق الحرج بالشخصيات التي انتحلوا صفتها مما يتسبب بتشويه سمعة الضحية و الإضرار به.

7 - كما أن بعض المخاطر على خصوصية الإنترنت سببها سجلات الخوادم التي تحتفظ بأرقام "الأي بي" الخاصة بالمستخدمين الذين اتصلوا بهذا الخادم؛ والكوكيز (كوكيز) التي تحتفظ بها مواقع الويب في العادة لتسهيل التصفح وحفظ تفضيلات ومعلومات المستخدم.

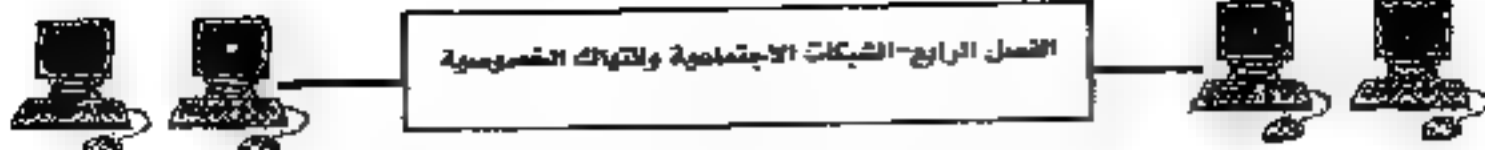
8 - برامج التجسس (Spyware) التي تهدف للتجسس أو التنصت على بيانات المستخدم أو اتصالاته.

و أخيراً نلاحظ أن القاسم المشترك بين كل هذه التهديدات هو ثقة المستخدمين العمياء في التطبيقات الاجتماعية. تماماً مثل البريد الإلكتروني عندما أصبح شائعاً، استغلت عصابات الجريمة المنظمة "الامكانيات المتاحة في وسائل الإنترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية بيسر وسهولة".

أصبحت شبكات التواصل الاجتماعي التي يظن الناس أنها عالم مثالي يتفاعل فيه الأشخاص بشكل ودي واجتماعي ويتبادلون فيه الصور وتفاصيل حياتهم اليومية عرضة للعيون المتطفلة ذات النوايا التي يشوبها الخبيث.

واستغلت هذه المواقع الاجتماعية مثل فيسبوك ومايسبيس وتويتر وغيرها في عمليات احتيال وابتزاز واختطاف وإساءة نتيجة استغلال المعلومات التي تعرضها.





ورغم وجود أفعال إلكترونية وآليات أخرى لتأمين هذه المواقع توجد حيل يمكن من خلالها لأطراف ثالثة الحصول على المعلومات الخاصة واستخدامها في أغراض غير مشروعة مما يعرض الأمن الشخصي للأفراد للخطر.

وحذر قرار حول حماية خصوصية الشبكات الاجتماعية وافقت عليه 37 دولة في ستراسبورغ الفرنسية عام 2008 من إمكانية تعريب البيانات الشخصية المتاحة على الصفحات الشخصية بهذه الشبكات عندما تفهرس باستخدام محركات البحث.

وجاء في القرار أن هذه البيانات يمكن استخدامها لارتكاب جرائم مثل الابتزاز والاختطاف إلى جانب التعرف على الجهات التي يمكن سرقتها وكذلك ارتكاب الأفعال الإباحية والاستغلال الجنسي والاحتيال المصرفي وغير ذلك من الجرائم.

التقنيات الحديثة و الخصوصية

تمكن تقنية المعلومات الجديدة تخزين واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم جمعها من قبل المؤسسات والدوائر الحكومية أو من قبل مؤسسات القطاع الخاص، ليس هذا فحسب بل يمكن مقارنة المعلومات المخزنة في قاعدة بيانات ما بمعلومات في قاعدة بيانات أخرى، ويمكن نقلها عبر البلد في ثوان ويتكاثف منخفضة نسبيا. "أن هذا بوضوح يكشف إلى أي مدى يمكن أن يكون تهديد الخصوصية" والحقيقة أن استخدام وسائل التقنية العالية في ميدان جمع ومعالجة البيانات الشخصية من قبل الدولة أو القطاع الخاص، قد عمق التناقضات الحادة التي برزت منذ القدم بين حق الأفراد في الحياة الخاصة، وموجبات اطلاع على شؤون الأفراد .



وتتمثل هذه التناقضات، بمعالم أربعة رئيسية:-

أولا :- التناقض بين حق الحياة الخاصة وحق الدولة في الاطلاع على شؤون الأفراد، والذي عمقه تزايد تدخل الدولة في شؤون الأفراد، وليس المراد بهذا التدخل الاطلاع على معلومات معينة عن الأفراد لتنظيم الحياة الاجتماعية على نحو افضل، كالاحتفاظ بسجلات الولادات والزواج والوفيات والإحصاءات وغيرها، بل استخدام الدولة للمعلومات الشخصية الخاصة بالفرد لأغراض تتناقض مع صونها واحترامها.

ثانيا :- التناقض بين حق الفرد في الاحتفاظ بسريته، ومصلحته في كشف حياته الخاصة ليتمتع بشار هذا الكشف. ورغم أن هذا التناقض للوهلة الاولى غير متحقق، باعتبار أن الاحتفاظ بالسرية حق، والكشف الطوعي عن هذه السرية حق أيضا، إلا أن احتمال استغلال المعلومات المعطاة طوعا لأغراض غير التي أعطيت لأجلها يمثل انتهاكا لحرمة الفرد وسريته.

ثالثا :- التناقض بين الحياة الخاصة، والحق في جمع المعلومات لغيات البحث العلمي، أو حرية البحث العلمي.

رابعا :- التناقض بين الحق في الحياة الخاصة وبين حرية الصحافة وتبادل المعلومات وهي ما تعرف بالحرية الإعلامية.

وإذا كانت الجهود التنظيمية، الإدارية والتشريعية، سعت الى إقامة التوازن بين هذه الحقوق المتعارضة فإن استخدام التقنية في ميدان جمع ومعالجة البيانات الشخصية، قد خلق واقعا صعبا هدد هذا التوازن من جهة وعمق حدة التناقضات المشار إليها من جهة أخرى.

فاستخدام الحواسيب في ميدان جمع ومعالجة البيانات الشخصية المتصلة بالحياة الخاصة للأفراد خلف آثارا إيجابية عريضة، لا يستطيع أحد إنكارها خاصة في مجال تنظيم الدولة لشؤون الأفراد الاقتصادية والاجتماعية والعلمية، وغيرها، وهذا ما أوجد في الحقيقة ما يعرف ببنوك المعلومات Data Bank والتي قد تكون مقصورة على بيانات ومعلومات تتصل بقطاع بعينه، كبنوك المعلومات القانونية مثلا، أو قد تكون شاملة لمختلف الشؤون والقطاعات، وقد تكون مهياة





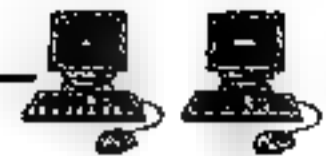
للاستخدام على المستوى الوطني العام أو المستخدمة على نحو خاص، كمراكز وبنوك معلومات الشركات المالية والبنوك وقد تكون كذلك مهياة للاستخدام الإقليمي أو الدولي.

وبفعل الكفاءة العالية لوسائل التقنية والإمكانات غير المحدودة في مجال تحليل واسترجاع المعلومات، اتجهت جميع دول العالم بمختلف هيئاتها ومؤسساتها الى إنشاء قواعد البيانات لتنظيم عملها، واتسع على نحو كبير استخدام الحسبات الآلية لجمع وتخزين ومعالجة البيانات الشخصية لأغراض متعددة فيما يعرف ببنوك ومراكز المعلومات الوطنية، وصاحب هذا التوجه ظهور الشعور بمخاطر تقنية المعلومات وتهديدها للخصوصية. هذا الشعور نما وتطور بفعل الحالات الواقعية للاستخدام غير المشروع للبيانات الشخصية واتساع دائرة الاعتداء على حق الأفراد في الحياة الخاصة مما حرك الجهود الدولية والإقليمية والوطنية لإيجاد مبادئ وقواعد من شأن مراعاتها حماية الحق في الحياة الخاصة وبالضرورة إيجاد التوازن بين حاجات المجتمع لجمع وتخزين ومعالجة البيانات الشخصية، وكفالة حماية هذه البيانات من مخاطر الاستخدام غير المشروع لتقنيات معالجتها.

يرى خبراء تقنية أن خصوصية المعلومات تمثل إحدى الحقوق المتزايدة الأهمية في عصرنا الحاضر. خاصة في إدارة بيانات المؤسسات والإدارات الحكومية، وكذلك الخاصة التجارية وحتى مواقع التواصل الاجتماعي عبر شبكة الإنترنت والتي لم تسلم جميعها من الاختراقات وانتهاكات الخصوصية.

ويؤكدون أن التقنية وابتكاراتها هي ذاتها من سهل عمليات انتهاك الخصوصية عبر الإنترنت، داعين الى استثمار التقنية في تعزيز أنظمة الحماية والأمان وتطويرها للحد من منع صلاحية الإطلاع على المعلومات والبحث فيها بدون حاجة، وعدم التمكين تقياً من نسخ البيانات الخاصة ومن ثم تداولها. فقد تصاعد عدد المخترقين Hackers، و سارقي الهويات Identity Theft، في الآونة الأخيرة سواء المتعلقة بالأشخاص أو الشركات والمواقع الكبرى ذاتها، مثل الفيسبوك وجوجل وسكايب و سوتي وغيرها والتي تعرضت إما لعمليات اختراق لخصوصية البيانات من



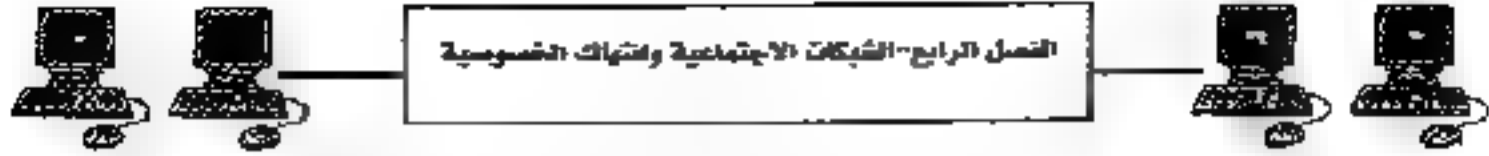


قبل مخترقين أو قامت باستغلال هذه البيانات لأهداف خاصة قد تكون إيجابية بالنسبة لها

وأفاد خبير تقنية المعلومات سامي العمودي، « أن اختراق البيانات يتركز في عدة طرق منها . محركات البحث «Search Engine»، وهي المواقع أو البرامج التي تتيح لمستخدمي البحث عن المعلومات في شبكة الانترنت، مثل «Google» و «Yahoo» و «AltaVista» و «Infoseek» و «Hotbot» وغيرها من محركات البحث، و بإمكان مستخدمي هذه المحركات، البحث عن المعلومات الشخصية لأشخاص آخرين. فإذا ظهر اسم المستخدم في إحدى صفحات الانترنت وبإمكان هذه المحركات البحث عن هذا المستخدم بين مليارات المواقع على شبكة الانترنت والكشف عن المعلومات الشخصية التي قد يظنها الشخص أنها محمية أو غير مكشوفة للكل». ويؤكد العمودي «أن التجارة الالكترونية «e-Commerce» لها النصيب الأكبر في التأثر بانتهاكات الخصوصية، أي عند شراء أي شيء عن طريق الانترنت، فهذا يعني أن المستخدم سيقوم باستخدام البطاقة الائتمانية للدفع، وهذا يعني إرسال رقم البطاقة الائتمانية عبر قنوات الانترنت، ومن الأنظمة الأمنية واسعة الانتشار حالياً لتشفير هذه الأرقام هي طبقة المقياس الآمن «Secure Socket Layer SSL»، والتي تدعمها أغلب برامج التصفح، ولكن يوجد سبب آخر للقلق حيالها، وهي طريقة تخزين هذه الأرقام في قواعد بيانات الشركات التجارية التي تتعامل بالتجارة الالكترونية».

وقال العمودي: « إن رسائل البريد الإلكتروني تعتبر الأكثر انتشاراً في وقتنا الحالي. فعند إرسال بريد إلكتروني قد يقوم أي شخص باعتراض خط الاتصال وقراءة الرسالة، خاصة إذا كان نص الرسالة غير مشفرة «Plain Text»، وقد لا يكون هذا الأمر ذات أهمية عند البعض بقدر أهميتها عند إرسال نصوص سرية لا يمكن قراءتها إلا للأشخاص الموجهة لهم هذه الرسائل الخاصة ». من جانبه قال محمد عمر الخبير في الشبكات وأمن المعلومات: «إن طرق حماية البيانات الأكثر استخداماً من قبل الشركات والمواقع تتركز على التشفير «Encryption» لحماية



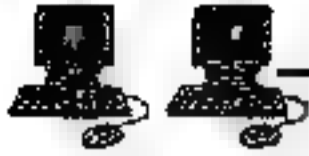


البيانات، و التي تحمي البريد الإلكتروني والتراسل عبر الشبكة بطريقة معينة. وتقوم تقنيات التشفير بتقديم آليات لحاكة التوافق على المستندات الالكترونية. طرق حماية البيانات الأكثر استخداما من قبل الشركات والمواقع تركز على التشفير «Encryption»، و التي تحمي البريد الإلكتروني والتراسل عبر الشبكة بطريقة معينة وتقوم تقنيات التشفير بتقديم آليات لحاكة التوافق على المستندات الالكترونية.

وأفاد « أن طريقة تسجيل نقرات لوحة المفاتيح «KeyLogger»، وهي برامج أو أجهزة مراقبة، لها إمكانية تسجيل النقرات على لوحة المفاتيح والتقاط صور لشاشات العرض والقيام بتخزينها في ملفات التسجيل «Log files»، مع إمكانية التوثيق لهذه البيانات، من دون علم المستخدم و تستخدم هذه الأداة لمراقبة الأجهزة عبر الشبكة، إذ تقوم بعض الشركات بمراقبة بعض الموظفين للتأكد من عدم إرسالهم لبيانات خاصة بالمنشأة إلى المنافسين أو بيعها لأغراض خاصة. لكن إن تم استخدامها من قبل أشخاص غير مصرح لهم فسيكون بإمكانهم الكشف عن البيانات والوصول إلى أدق إحصائيات الاستخدام عبر الشبكة». وأشار إلى أن الأفراد في إدارتهم لتعاملهم الخاص عبر الإنترنت يمكنهم استخدام وسائل جديدة لحماية خصوصياتهم، مثل البريد المتخفي «anonymous mailers»، والمتصفحات التي تسمح بالتجول دون كشف الهوية عبر الإنترنت عبر التصفح الخاص «privet browser».

وقال عصام الأحمد مصمم ومبرمج مواقع الإنترنت: « إن مواقع الإنترنت تستخدم نظم «UPS» إضافة إلى نظم التدعيم والتي تعتبر تقنيات متعارف عليها لتأمين المعلومات مثل تقنيات الجدار الناري وإجراءات التحكم بالدخول والتشفير وذلك حتى يمكن توفير الحماية الملائمة للمعلومات السرية من أي دخول غير مصرح به»

وأضاف: « إن النتيجة عند الدخول في الشبكات الاجتماعية بأسماء محتلمة أو بإدخال بيانات غير صحيحة أمر يمكن اكتشافه، ويمكن تكوين صورة عن المستخدم واهتماماته. وذلك باستخدام خوارزميات التقنيات الحديثة، من تقليب



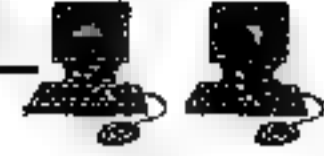
البيانات « Data Mining » ودراسة وتحليل السلوكيات لدى المستخدمين وغيرها». وحتم الأحمدي قائلا : « لم نصل إلى حالة حفظ الخصوصية و لأمان الكاملة حتى الآن. فهناك نزاع بين خبراء أمن المعلومات ومنتھكي خصوصية البيانات والمخترقين فعلى الشركات والمواقع والبنوك خاصة في الوقت الحالي محاولة تطوير أنظمة الأمان لديها لتجنب الوقوع فيما وقعت فيه الكثير من الشركات والمواقع في الفترة الأخيرة».

وفي الحقيقة أن الجرائم المعلوماتية هي ثمرة من ثمار التقدم السريع في شتى المجالات العلمية الذي يتميز به عصرنا الحاضر ؛ فهناك ثورة في مجال الجينات والصنفيات نتيجة للتقدم في فرع الهندسة الوراثية ؛ وهناك ثورة في مجال وسائل الاتصال والمعلومات Information Revolution ترجع إلى استخدام الكمبيوتر (الحاسوب) ... الخ.

ولقد صاحب هذا التقدم السريع في مجال العلوم والتقنية واستخداماتها لخير بشرية ؛ تقدم آخر مواز في مجال الجريمة ؛ فلم تصبح الجريمة مقصورة على طبقة معينة من طبقات المجتمع دون أخرى ؛ وذلك لوضوح إجرام الفساد الذي يتورط فيه كبار المسؤولين في الدول المختلفة ؛ علاوة على إجرام ذوي الياقات البيضاء ؛ الذي يتورط فيه كبار المسؤولين في الشركات العملاقة ؛ وإجرام الاتجار بالمخدرات.

وعلى مستوى ثورة الاتصال والمعلومات نجد أن الصراع مستمر بين جانبي الخير والشر في هذه الثورة ؛ ففي جانب الخير نجد أن هذه الثورة ساعدت على عولمة المعلومات ؛ وتسهيل كثير من الخدمات والأعمال ؛ فقد توصلت البشرية إلى السيطرة على المعلومات من خلال استخدام الحاسب الآلي computer لتخزين ومعالجة واسترجاع المعلومات ؛ فضلا عن استخدامه في عمليات التصميم والتصنيع والتعليم والإدارة ؛ دھيك عن تطوير تطبيقاته لتشمل أداء خدمات عديدة مثل التعليم والتشخيص والخدمات التمرضية وتسهيل المعاملات والخدمات البنكية والحجز





الآلي لنقل الأشخاص وإدارة المكاتب الحديثة وقيادة المعارك ؛ وعلى وجه العموم دخل الحاسب الآلي في شتى نواحي الحياة الإنسانية .

فضلا عن أنه جعل المعلومات في متناول الجميع من خلال شبكات الإنترنت ، أي شبكات المعلومات المحلية والإقليمية والعالمية ؛ وأصبح العالم بذلك مردخراً بكم هائل من المعلومات لا تعرف الحواجز الجغرافية ولا المسافات ؛ بصورة يمكن معها القول بأن العالم صار أشبه بمجتمع كبير مترابط فيه الحاسبات و شبكات المعلومات : نعلن بزوغ فجر ثورة جديدة هي الثورة المعلوماتية La revolution informatique أو الثورة الصناعية الثالثة التي تدفع بالإنسانية إلى عصر جديد هو عصر أو مجتمع المعلومات .

وعلى جانب الشر نجد أن الإنسان - متأثر بنزواته وشهواته ونواقصه - يسيء استخدام ثورة الاتصال والمعلومات : فإذا كانت الكثير من المؤسسات كالبנק والشركات الكبرى تستخدم الحاسب الإلكتروني ؛ فإنه من خلاله ترتكب كثيراً من الجرائم مثل السحب الإلكتروني من الرصيد بواسطة الصكارت الممغنط إذا كان مزوراً أو من غير صاحب الصفة الشرعية. كذلك يمكن تصور التجسس عن بعد وسرقة بيانات تتعلق بالأمن القومي ؛ ومن الممكن أن يترتب على الإصابة بالفيروس المعلوماتي تدمير برامج مهمة ، علاوة على أنه من المتصور أن يحدث مساساً بحياة الأفراد الخاصة وانتهاكها من خلال استخدام الحاسب الآلي وشبكة الانترنت والمثل يقال بالنسبة للجرائم الماسة بالآداب .

القرصنة على الفيس بوك

توقع خبراء في قطاع المعلوماتية أن يكون الهجوم الأخير الذي نمذه قرصنة عبر موقع "Facebook" الواسع الانتشار من خلال صفحات مرفقة تقلد صفحة الموقع الرسمية مقدمة لموجة من الهجمات الجديدة، وذلك رغم ما يعرف عن القائمين على الموقع محاربتهم للقرصنة.





واعتبر الخبراء أن هذا التركيز المتوقع على "Facebook" يعود إلى تحويل القراصنة أنظارهم نحو مواقع التعارف التي تضم ملايين المشتركين، عوضاً عن قرصنة البريد الإلكتروني العادي.

وقال مايكل أرجست، وهو محلل شؤون أمنية في شركة "سوفوس" للمعلوماتية: "في العقد التاسع من القرن الماضي، كان القراصنة يستخدمون البريد الإلكتروني، أما اليوم، فالهدف هو مواقع التعارف."

وشرح أرجست رأيه قائلاً، "إن الناس اعتادوا على عدم التعامل مع الرسائل الإلكترونية المشبوهة التي تردهم، غير أنهم لا يفعلون ذلك على مواقع التعارف مثل "Facebook" أو Twitter مما يفسر ارتفاع هجمات القرصنة على تلك المواقع، التي تعرضت خلال الأشهر الثلاثة الأولى من العام الجاري إلى 6400 هجوم، مقابل 11 ألف هجوم للعام 2008 ككل." بحسب سي ان ان.

وترى بعض شركات الأمن الإلكتروني أن طابع مواقع التعارف تمنح المشتركين فيها شعوراً مزيفاً بالأمان، وذلك على اعتبار أن كل مشترك يتعامل حصراً مع مجموعة من الأصدقاء ضمن شبكة واحدة، ويفترض بالتالي أن كل ما يردده منهم هو موضع ثقة.

ورغم أن اختراق موقع "Facebook" لا يضمن للقراصنة مكاسب مالية مباشرة، إلا أنهم يسعون للحصول على كلمات السر الخاصة بالمستخدمين لإدراكهم بأن الكثيرين يعمدون إلى استخدام كلمة سر بعينها لكل المواقع التي يستعملونها، بما في ذلك حساباتهم المالية.

ويمتلك موقع "Facebook" جهازاً أمنياً متخصصاً، يقوم بمسح حركة المشتركين، وذلك من خلال التدقيق بعند الرسائل التي تصدر من كل حساب، فإذا ما رصدوا حركة مفرطة من حساب معين يقومون بإصدار صاحبه ناحتال تعرضه للقرصنة، "وفقاً لما أوردته مجلة "تايم".

وكان موقع "Facebook" قد تعرض للقرصنة الأسبوع المتصرم من حلال ظهور صفحة رئيسية مزيفة لخداع المشتركين به تسمح للقراصنة بالحصول على





كلمات السر الخاصة بالمستخدمين، والتسلسل إلى حساباتهم لدعوة المزيد من الأشخاص لدخول الصفحة المزيفة.

مواقع التعارف... طريقة جديدة لاختراق الخصوصية

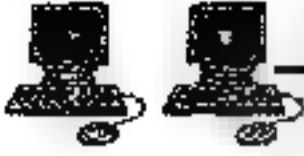
انتشرت الشبكات الاجتماعية على الإنترنت كـ "فايسبوك" و"غوغل بلس" و"تويتر" وغيرها وزاد روادها على اختلاف أعمارهم وأذواقهم بشكل كبير وهو ما وجد فيه القراصنة هدفاً سهلاً لتحقيق مآربهم، لذلك نصح خبراء في مجال الأمن الإلكتروني مستخدمي مواقع التعارف الاجتماعي بضرورة توخي الحذر عند تلقي رسائل تتضمن دعوات للانضمام إلى أماكن أخرى. كما وحذر الخبراء من الوقوع في شباك ما أطلقوا عليه "الجريمة المنظمة" عبر كشف معلومات قيمة وتبادل العناوين الصحيحة وحتى أرقام بطاقات الائتمان والحسابات المصرفية، لأن هذه المواقع سهلة الاختراق ويمكن أن تستخدم للابتزاز.

تزايدت أعداد مرتادي الشبكات الاجتماعية أو ما يعرف بمواقع التعارف، بشكل لافت العام الماضي، الأمر الذي أتاح لقراصنة الإنترنت فضاءً واسعاً سمح لهم بإبراز مهاراتهم من خلال انتهاك الخصوصية وإلحاق الضرر بالمستخدمين، خصوصاً الأطفال والمراهقين، الذين بات ارتيادهم تلك الشبكات أمراً يستدعي تحركاً عاجلاً.

خصوصاً بعد تعرض عدد كبير من الأطفال دون 16، إلى احتيال واستغلال من طرف القراصنة. لذلك نصح خبراء في مجال الأمن الإلكتروني مستخدمي مواقع التعارف الاجتماعي بضرورة توخي الحذر عند تلقي رسائل تتضمن دعوات للانضمام إلى أماكن أخرى.

ورغم الإيجابيات التي تحملها الشبكات الاجتماعية، من خلال تقريب الشعوب من بعضها، وفتح آفاق جديدة أمام المستخدمين، إلا أن الخبراء يرون فيها وسيلة للتحكم عن بعد، في أجيال كاملة، ورصد طرق تفكيرها وتوجهاتها.





إضافة إلى ذلك تعتبر المواقع الاجتماعية بمثابة فضاء افتراضي، لا يعرف أحد هوية الآخر وحقيقة نواياهم. ومن ثم ينصح المختصون بعدم وضع صور خاصة أو عائلية على الشبكة، حيث يمكن استغلالها بطريقة سيئة.

يستطيع المحترفون الدخول إلى الحسابات الشخصية على مواقع التعارف بكل سهولة نظراً لتمكّنهم من فك كلمات السر. ومن خلال مسح شمل آلاف المستخدمين في أوروبا تبين أن معظم رواد الشبكات لا يكتثرون بتأمين حساباتهم، نظراً لقلة أهميتها، حسب رأيهم.

ومن ثم كان من السهل اختراقها من طرف القراصنة لذا وينصح المختصون باختيار كلمات سرية صعبة ومعقدة لتفادي انتهاك الخصوصية. وتخضع المواقع المذكورة لقوانين البلدان التي تطلق منها، أو الدول التي تمتلك فيها فروعاً

وموقع «فيس بوك» الشهير لا يمتلك فرعاً في ألمانيا، مثلاً، رغم وجود نسخة ألمانية منه، وبالتالي فإن أي سوء استخدام وانتهاكات تخضع لقوانين ولاية ديلوير في الولايات المتحدة. ويتوقع الخبراء حالياً أن هذه المواقع، خصوصاً الشهيرة منها، ستصبح من أهم أهداف القراصنة في عام 2008.

وتم وضع فيروسات في بعض صفحات موقع «ماي سبايس» مصممة لاستغلال إحدى الثغرات الأمنية في نظام «ويندوز» و«إنترنت إكسبلورر»، التي قامت مايكروسوفت بمعالجتها أخيراً وتبدأ عملية الاحتيال بعرض فيلم فلاش يتم تنصيبه في صفحتين من صفحات الموقع التي تقود المستخدمين إلى صفحة تسجيل دخول وهمية، وهذه الصفحة بدورها تقوم بتحميل فيروسات عدة خبيثة تحصل على كلمات السر وأسماء الدخول الخاصة بالزائرين.

ودعا مسؤولون بريطانيون إلى تشديد الرقابة على المواقع الاجتماعية، بعد شيع ظاهرة ارتياد أطفال، ما بين 10 و13 عاماً، بعض الشبكات المعروفة مثل «ماي سبايس».





والخطير في المسألة تعليم الأطفال كيفية الكذب في ما يخص أعمارهم، لأن غالبية المواقع تفرض قيوداً معينة على المستخدمين، خصوصاً في ما يخص لعمر وينصح الخبراء في الشبكات الاجتماعية، المستخدمين الصغار توخي الحذر عند إبحارهم في قضاء الشبكات الفسيح، لأنهم لا يعرفون من سيلتقون في أول منعطف.

ومن جهة أخرى طالب مختصون في بريطانيا بتحديد عمر المستخدم بـ 14 سنة، كأدنى حد إلا أن خبراء أمن الإنترنت حذروا من الوقوع في شرك ما أطلقوا عليه «الجريمة المنظمة» عبر كشف معلومات مهمة وتبادل العناوين الصحيحة وحتى أرقام بطاقات الائتمان والحسابات المصرفية، لأن هذه المواقع سهلة الاختراق ويمكن أن تستخدم للابتزاز، خصوصاً أن التكنولوجيا المستخدمة فيها تسهل على العصابات استهداف بعض البسطاء وقد تُعرض حتى الأطفال للخطف، فليس مستخدم الإنترنت العادي وحده من يجب المواقع الاجتماعية، بل القراصنة أو «مجرمو الشبكة» أيضاً.

أشارت دراسة بريطانية حديثة شملت 3000 طفل، ما بين الثامنة و11 من العمر، إلى أن معظمهم لديه حساب على أحد المواقع المشهورة. الأمر الذي يتنافى مع شروط تلك المواقع. وقال باحثون في مركز حماية الأطفال من الاستغلال الرقمي، إن غرف الدردشة وبرامج المراسلة الفورية، باتت وجهة مفضلة لدى كثير من الأطفال. وأشار المركز إلى أن حالات سوء المعاملة، التي تعرض إليها أطفال دون الـ 16، تبقى محدودة حتى الآن.

حماية خصوصية مستخدم الشبكات الاجتماعية

وللحيلولة دون انتهاك الخصوصية في الشبكات الاجتماعية فلا بد من اتباع النصائح الآتية:-

- 1 الاختيار الدقيق للمعلومات الحساسة التي تكتبها أو الصور و الفيديوها التي ترفعها على حسابك فلا تكتب أي شيء في صفحة الملف الشخصي، لوحة





الإعلانات، والرسائل الفورية أو أي نوع آخر من أشكال المشاركة و المشر الإلكتروني على الانترنت من شأنه أن يعرضك لإمكانية سرقة الهوية أو التهديدات الأمنية. وهذا يتضمن الأسماء الشخصية والتجارية والعناوين وأرقام الهاتف، والمسميات الوظيفية، وتواريخ الميلاد، وتفاصيل حدودك الزمني، والأعمال الروتينية اليومية أو معلوماتك الأسرية. فمن الأهم أن تحتفظ بهذه المعلومات بدلاً من أن تستخدم ضدك يوماً ما.

2 - الحذر عند قبول طلبات الصداقة و التحقق ممن أرسل الطلبات و معرفة أنك لست ملزماً بمصادقة كل من طلب منك ذلك.

3 - الحذر عند إعطاء الصلاحيات للبرامج و قراءة ما التراخيص التي يريد البرنامج و لا تثق بكل البرامج و التطبيقات فبعضها وجد بغاية أخذ معلوماتك و معلومات أصدقائك.

4 - من البديهي أنك يجب أن تضبط إعدادات الخصوصية حسب ما يناسبك و أن لا تعطي الكثير من المعلومات الشخصية عنك للعموم.

5 - الأهم حماية كلمة السر و الحذر من التروجان و الفيروسات و الحيل التي وجدت بفرض سرقة كلمات السر مثل أن يدعي شخص أنه ممثل الدعم في شركة الفيس بوك و يطلب منك أن تصفح على رابط مرسل بالإيميل يطلب منك فيه تعديل معلوماتك لضمان عدم إغلاق حسابك، و لو دقت في الرابط المرسل بعد الضغط عليه تجده ليس للفيس بوك، مثلاً ممكن أن يكون facebook أو facebook أو ما شابهها من الصاب، وأمثلة أخرى مهمة facebook.somedomain.com و هنا يجب الحذر أن الموقع الرئيسي المرسل هو somedomain.com مثلاً و ليس facebook و الفيس بوك هنا عبارة عن مجلد فرعي فيه، و تكون واجهة الموقع المرسل عبارة عن واجهة مطابقة 100% لواجهة الموقع المراد سرقة كلمة سره، و لكن عند إدخال اسم المستخدم و الإيميل يقوم هذا الموقع المزيف بإرسال معلوماتك للمخترق بدلاً من إدخالك للموقع، هذا ما يسمى الصيد أو phishing





6 - الضغط الدائم على الشبكات الاجتماعية كي تعطي المزيد من الخصوصية للمستخدمين.

7 - عدم نشر ما قد يسيء إليك.

8 - القيام بضبط وتعديل إجراءات الحماية الخاصة بالخصوصيات في الشبكات الاجتماعية.

9 - تأكد من إرسال معلوماتك الشخصية عبر اتصال آمن، فإدى إرسال أرقام بطاقة التأمين، أو المعلومات المصرفية، أو كلمات السر، تحقق من وجود صورة قفل على شريط عنوان المتصفح. فمثل هذه التقنية تقوم بتشفير البيانات التي ترسلها وتتلقاها، مما يجعل من الصعب على أي شخص التجسس على الخط للوصول إلى هذه المعلومات.

10 - الهروب من تعقب الإعلانات لك، فغالباً ما تقوم شبكات الإعلانات بتجميع ملف صيفر على كومبيوترات الأشخاص الذين يقومون بزيارة مواقع شبكية معينة.

11 - يجب على كل من يدخل ويتصفح الإنترنت أن يكون لديه أربعة أنواع من البرامج وهي: مضاد فيروسات قوي، فاحص وماسح برامج التجسس والكوكيز، فاحص وماسح أحصنة طروادة Trojan، كما عليك تحديث هذه البرامج كل شهر وأخيراً تجنّب الدخول بكثرة الى المواقع التجارية التي تقدّم خدمات مجانية.

ورداً كنت تستخدم خطاً سريعاً مثل ADSL أو DSL فأعلم بأن نسبة الخطورة أكثر ونسبة إصابتك أكبر ممن يستخدمون الخطوط البطيئة. فكن حذراً حتى لا تقول وداعاً للخصوصية.

12 - كن متشككاً بما تستقبله من معلومات فمواقع الشبكات الاجتماعية مليئة بالمعلومات التجارية المفيدة، فضلاً عن كميات كبيرة من التضليل عديم الفائدة. فكر بمصادقية و واقعية في كل ما تقرأه في الإنترنت سواءً كانت نصائح لمضاربي الاسهم، أو الأخبار العاجلة، أو فضائح سياسية أو إشاعات





منتشرة. فبعض الناس سوف يكذب من أجل كسب مصلحة خاصة فيهم، والبعض الآخر قد يكون مجرد بغاء لا يعي مايردده من القيل و القال.

13 - كن عميق التفكير فلا أحد يحب كثير الكلام أو من يتكلم بما لا يعرف أو يدعي ما لا يملك، ولكن في الإنترنت قد يخلع بعض الأشخاص الأقنعة المزيفة التي كانوا يرتدونها في الحياة الواقعية ليظهروا على حقيقتهم، فمن أسهل الأشياء في الإنترنت ومن ضمنه الشبكات الاجتماعية التحضي خلف الأسماء المستعارة.

و الخوض في كل شيء محذور من الكذب و الفحش و نشر الفضائح فتجنب زلات لوحة مفاتيحك ولا تكتب أي شيء يمكن أن يضرك فيما بعد، و فكر مرتين قبل الكتابة. قال تعالى: ﴿مَا يَلْفُظُ مِنْ قَوْلٍ إِلَّا لَدَيْهِ رَقِيبٌ عَتِيدٌ﴾ (سورة ق الآية 18)

14 - كن ذواقاً مهنياً فإذا أردت نشر صورة أو فيديو أو حتى كتابة رسالة في الشبكات الاجتماعية فتأكد من أنه سيظهر في أجمل شكل ممكن لأنه في النهاية يعبر عنك و عن آرائك و معتقداتك. فلا تظهر بشكل مخل بالأدب و لا ترتدي قبعة المهرج.

15 - كن متيقظاً فطناً فالكثير من الناس في الشبكات الاجتماعية قد يظهرون بصورة مغايرة تماماً لواقعهم فإذا كنت تدرش مع المدير التنفيذي لشركة مرموقة ففي الواقع قد تكون تتحدث إلى طفل مراهق أو سجين محكوم عليه بالإعدام. فتأكد دائما من هوية الأشخاص الذين تتعامل معهم و أبحث عنهم و تحقق من المعلومات التي يرسلونها لك.

الخصوصية الشخصية الخاصة أو الخصوصية الاعتبارية للمواقع من الحقوق المحفوظة والتي يعتبر الاعتداء عليها جرماً يستحق صاحبها العقاب والتجريم، وقد أدى انتشار الشبكة وخاصة الاجتماعية - بما تحمله من خصوصية





اجتماعية للشخص والمواقع - إلى سهولة هتك ستار الحقوق والتلاعب بها إما بالتعطيل أو التغير أو بالاستغلال السلبي لها ومعلوماتها.

وانتهاك الخصوصية يتم ذلك من عدة طرق، منها انتحال الشخصية الخاصة للأفراد أو الاعتبارية للمواقع والشركات، فلكل شخصية فردية واعتبارية حقوقها المحفوظة، وخاصة الشخصيات المهمة والمتميزة وأصحاب الرئاسات الكبرى، وكذلك الحال مع المواقع الشهيرة والمتميزة، استغلالاً للنفوذ والشهرة والثقة الاعتبارية لكثير من الشخصيات والمواقع.

ولتأمين الحقوق الخاصة للأفراد والمواقع، لابد من معرفة ما يلي: -

- 1 - ليس كل ما يعرف يكتب على الحاسب وينشر على الشبكة، فحاول أن تكون لك أسرارك الخاصة التي تحتفظ بها في غير جهاز الحاسب، أو اجعل لها جهازاً خاصة لا يكون متصل بالشبكة.
- 2 - شفر معلوماتك الخاصة، أي اجعل لها شفرة خاصة من رقم أو نحوه يصعب تخمينها، وحاول تغييرها كل فترة معينة، والبرامج التي تخدم في التشفير كثيرة.
- 3 - اعرف من تضيفهم كأصدقاء أو مشاركين ومطلعين على ملفاتك ومعلوماتك.
- 4 - اعط صلاحية خاصة لأشخاص معروفين بالاطلاع على الملفات الخاصة، أو استخدامها في أضيق نطاق ممكن.
- 5 - احتفظ بنسخ احتياطية من أعمالك أو موقعك أو بياناتك في مكان آمن لا يصل له غيرك أو من تخوله بذلك تحت إشرافك.
- 6 - طور من إمكانيات التقنية والبرمجية واعتمد في الغالب - بعد الله سبحانه وتعالى - بنفسك أو من تثق بهم.
- 7 - اختر شركات متطورة ومعروفة بنظام الحماية لديها حتى تنشئ موقعاً في مساحة آمنة بإذن الله تعالى.
- 8 - زود جهازك ببرنامج حماية قوي وفعال.





9 - داوم على الاطلاع على ملفاتك وتفقدها باستمرار ، أو وكل من تثق به في ذلك.

حقائق عن الخصوصية

هناك نوع من المعلومات يطلق عليها خاصة كونها تتعلق بالشخص ذاته وتنتمي إلى كيانه كإنسان مثل الاسم والعنوان ورقم الهاتف وغيرها من المعلومات، فهي معلومات تأخذ شكل بيانات تلزم الإلتصاق بكل شخص طبيعي معرف أو قابل للتعريف.

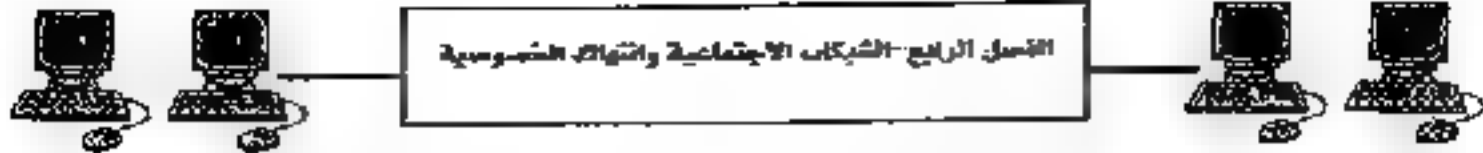
وهذه النوعية من المعلومات أصبحت في وقتنا الحاضر على درجة كبيرة من الأهمية في ظل فلسفة المعلوماتية المعاصرة، سيما وأن فكرة العالم الرقمي، لا يمكن لها السير في التطور ومواكبة اهتمامات الإنسان سوى باستخدام المعلومات. من هنا ظهر ما يعرف بالخصوصية المعلوماتية.

تعتبر الخصوصية على الإنترنت من القضايا الشائكة في أيامنا هذه وانتشرت في الآونة الأخيرة العشرات من برامج التجسس التي تقوم بجمع المعلومات عن جهاز الكمبيوتر وعن الشخص وإظهار العديد من الإعلانات على النوافذ المنبثقة. فضلاً عن هذا كله إنتشرت الديدان التي تعجز أقوى البرامج المضادة للفيروسات عن ردعها وتسبب العديد من الأضرار على جهاز الكمبيوتر، بالإضافة إلى أحصنة طروادة Trojan والهاكرز (Hackers).

1 - تقوم الشبكات الاجتماعية بإعطاء المعلنين معلومات عن جنسك و عمرك و مكان إقامتك و إهتماماتك و وظيفتك و معلومات عن أصدقائك و هذا يفرض إستهدافك بإعلانات هذه الشركات حسب ما يوافق رغبات الشركة المعنية.

2 - تقوم الشبكات الاجتماعية بالإحتفاظ بكل معلوماتك على سيرفرتها، فكل ما تكتب و كل ما تحمل من صور و فيديو هات تحتفظ به على سيرفرتها، و بالتالي من الممكن الإطلاع على هذه المعلومات من قبل





الموظفين في هذه الشركات مثلاً و من قبل السلطات في حال طلبت معلوماتك من هذه الشبكات الإجتماعية.

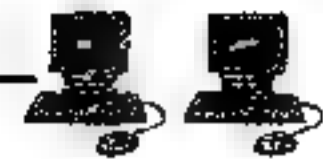
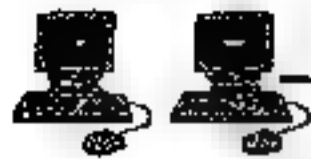
3 - بعض الشركات كالفييس بوك يحتفظ بصورك حتى بعد حذفها ، و بالتالي ما ترفعه على هذه الشبكات سيصبح ملكها و ليس ملكك، و أنت موافق على هذا عند الإشتراك بهذا الموقع، إذا قانونياً يحق لهذه الشبكات بيع صورك!

4 - تستغل هذه الشبكات عدم معرفة بعض الأشخاص بإعدادات الخصوصية و بالتالي تقوم بوضع أخف إعدادات عند إنشاء الحساب لأول مرة و بالتالي إذا لم تقم بضبط الإعدادات قبل البدء من الممكن أن يطلع كل الناس على كل ما - لا يمكنك التحكم الكامل بكل إعدادات الخصوصية في المواقع الإجتماعية كالفييس بوك، فمثلاً إذا كتبت تعليقاً على إحدى المواضيع فهذا التعليق سيعرض على حائطك و لا خيار مناسب لإخفاء كل المعلومات عن حائطك، كما أن الإجابة عن الأسئلة ستظهر في حائطك و لا وسيلة لإخفائها.

5 - من الممكن إستغلال بعض الثغرات و الأخطاء البرمجية في المواقع الإجتماعية أو إختراق حسابك للحصول على معلوماتك الشخصية.

هذه الحقائق تتطلب منا الحذر فيما نكتب و فيما نرفع على المواقع الإجتماعية و خصوصاً أن كل ما نرفع من وسائل في بعض الشركات يعتبر ملكهم و يمكنهم استخدامها و نشرها قانوناً.

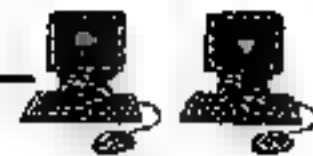
جميع الشبكات الاجتماعية لديها مبادئ معينة و قواعد محددة للمعلومات المنشورة قد تناسبك أو لا فخذ الوقت الكافي لقراءة و فهم هذه الوثائق، لأنها تتضمن أنواع المعلومات التي سوف تكشف عنك أو تباع لأطراف أخرى حدد ما يعجبك و ما لا يعجبك منها و على ذلك تعامل مع تلك الشبكة الاجتماعية.



هوامش الفصل الرابع:

- 1 - محمود البستاني: الاسلام وعلم الاجتماع، مجمع البحوث الاسلامية للدراسات والنشر - بيروت، الطبعة الأولى 1414هـ.
- 2 - صحيفة بوابة الشرق، عدد السبت 22 أكتوبر 2011.
- 3 - www.twitter.com
- 4 - www.adb.org/knowledgesolutions
- 5 - http://mubde3nt.net/news-40.html
- 6 - مشعل عبد الله القدهي: المواقع الإباحية على شبكة الانترنت وأثرها على الفرد والمجتمع، مدينة الملك عبد العزيز للعلوم والتقنية.
- 7 - علي بن عبد الله عسيوي الآثار الأمنية لاستخدام الشباب للإنترنت، ص 44.
- 8 - متفق عليه / البخاري، كتاب المناقب، باب علامات النبوة في الإسلام، حديث رقم (3411).
- 9 - مسلم، كتاب الإمارة، باب الأمر بلزوم الجماعة عند ظهور الفتن، حديث رقم (4890).
- 10 - متفق عليه / البخاري، كتاب النكاح، باب ما يتقى من شؤم المرأة، حديث رقم (4808).
- 11 - مشعل عبد الله القدهي: المواقع الإباحية على شبكة الانترنت وأثرها على الفرد والمجتمع، ص 5.
- 12 - الساحة العمانية، القرصنة الإلكترونية والهاكرز و كيفية الحماية - جديد العلم والمعرفة، 21-02-
http://www.oman0.net/showthread.php/432781,2010
- 13 - http://www.alriyadh.com/2011/07/20/article652259.html-
(هوثرور نايجل الوجه الآخر لشبكات التواصل الاجتماعية 20 يوليو 2011)
http://coeia.edu.sa/images/stories/PDFs/Privacy_in_social_networks.pdf





14 - المبارك نوف - الخصوصية في الشبكات الاجتماعية - 2011/12/2

http://www.alqabas.com.kw/Temp/Pages/2011/07/20/40_page.pdf

15 - كبي خالد - مخاطر التواصل الاجتماعي - 20 يوليو 2011

<http://www.tech-wd.com/wd/2010/05/24/control-your-privacy-on-facebook/>

16 - الضراب مازن - خصوصيتك تحت سيطرة الفيس بوك - 24 مايو 2010

17 - امن المعلومات انظر: - <http://security-sy.com/?p=451>

18 - نجران نيوز . 08 - 08 - 2011

سمورس: <http://www.sauress.com/najrannews/8632>

خراقة شيء اسمه أمن الإنترنت!

19 - الجزيرة نت . الاخبار تقارير وحوارات .

<http://www.aljazeera.net/news/pages/f2ad51ae-eb30-4af0-98c3-eb433b63fe12>

20 - عبد الله بن يحيى آل محيا: أثر استخدام الجيل الثاني للتعليم الالكتروني .

<http://www.facebook.com/profile.php?id=100002246432444>

21 - <http://www.thenewalphabet.com/radio/details3413.html>

22 - رؤوف أونلايس . منتديات الشروق . الفراغ التشريعي في مجال مكافحة

الجرائم الالكترونية 05 - 07 - 2007 . انظر: -

<http://montada.echoroukonline.com/showthread.php?s=ce1d1dec60d010e871230ecdce6e4360&t=7916> .

23 - المخاطر الامنية للانترنت . منتديات الشروق . 09 - 11 - 2008

<http://montada.echoroukonline.com/showthread.php?s=ce1d1dec60d010e871230ecdce6e4360&t=45297>





24 - موقع هيئة تقنية المعلومات ، سلطنة عمان . October 08, 2012

ابظر .

[http://www.ita.gov.om/TTAPortal_AR/Pages/Page.aspx?NID=1
&PID=8&LID=4](http://www.ita.gov.om/TTAPortal_AR/Pages/Page.aspx?NID=1&PID=8&LID=4)

25 - لأمارات اليوم ، التكنولوجيا الرقمية تواكب لتطور 4 / 9 / 2012

[http://www.emaratalyoun.com/local-section/2008-05-31-
1.199487](http://www.emaratalyoun.com/local-section/2008-05-31-1.199487)

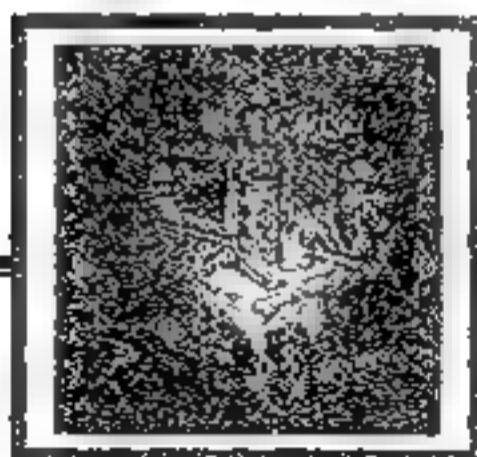




الفصل الخامس

الفرصنة الإلكترونية

في الدول العربية





سجلت عمليات القرصنة ارتفاعاً ملحوظاً في دول الشرق الأوسط وإفريقيا فقد وصلت نسبتها في مصر عام 2004م إلى 65 في المئة في حين بلغ حجم صناعة البرمجيات في نفس المنطقة 560 مليون دولار .

ثم عادت وانخفضت بمقدار 10 في المئة بحلول عام 2009م . فيما بلغ حجم صناعة تكنولوجيا المعلومات 1.1 مليار دولار. وإذا حدث نفس الانخفاض في منطقة الشرق الأوسط وإفريقيا فسيبلغ حجم الصناعة 27.5 مليار دولار مرتفعاً من 17 مليار دولار حالياً.

ويقدر عدد العاملين في قطاع تكنولوجيا المعلومات بالشرق الأوسط وإفريقيا 220 ألف شخص يعملون حالياً من بين تسعة ملايين يعملون في نفس القطاع حول العالم .

الهاكرز العربي

كثير من الناس في الدول العربية يرون بأن الهاكرز هم الأبطال . فمنذ دخول الإنترنت للدول العربية في تسعينيات القرن الماضي و الناس يبحثون عن طرق القرصنة الجديدة و كثير من الناس تعرضوا لهذه المشكلة .

آخر لإحصائيات ذكرت بأن هناك أكثر من 80 / من المستخدمين العرب أجهزتهم تحتوي على ملف الباتش و الذي يسهل عمل الهاكرز .

وتؤكد الدراسات ارتفاع نسبة الاختراقات في شبكة الإنترنت في المنطقة العربية بأكثر من 21% بعد زيادة نسبة مستخدمي الإنترنت العرب بحوالي 177% خلال السنوات الثمانية الماضية.

ففي منطقة الخليج العربية تزداد خطورة الجريمة الإلكترونية مع وقوع نحو أربعة آلاف هجوم إلكتروني في النصف الأخير من عام 2007 كان النصيب الأكبر منها للسعودية ثم للإمارات تليها الكويت .





فيما أعلن بنك دبي الإسلامي عن وقوع حالات سطو إلكتروني على حسابات بعض عملائه عبر بطاقة بنكية مزورة تم استخدامها من أحد البنوك الروسية ومن إحدى الحانات الأميركية فالعصابة الإلكترونية لا تعترف بحدود المكان والزمان، اللافت أن المجرم الإلكتروني يستخدم وسائل مبتكرة دوماً للإيقاع بصحته منها تصميم موقع مشابه لصفحة بنك ما يدخل إليها المستخدم الواهم واضعاً كل بياناته المصرفية ليقع ضحية سهلة للص في مكان ما في العالم.

وفي أحدث تقرير لشركة سيمانتيك المتخصصة في الحماية الإلكترونية ظهر أن القيمة الإجمالية للمسروقات المعلن عنها من خلال قنوات الاقتصاد السري على الإنترنت تجاوزت 276 مليون دولار خلال الفترة من يوليو عام 2007 إلى نهاية يونيو من العام الحالي فالخطر إذاً غير بعيد.

فقد كثرت في الفترة الأخيرة الاختراقات وبالذات في المنطقة العربية من خلال تويتر (الاختراقات في تويتر) لاسيما المواقع التابعة لبعض المؤسسات الحكومية وايضا عن اختراقات (هكر سعودي ينشر تفاصيل آلاف بطاقات الائتمان الإسرائيلية على الانترنت).

أما أشهر الأشخاص العرب الذين اشتهروا بالهكرز فقد جاء في الترتيب أربعة سعوديين وجزائري، وأغلب هجماتهم على المواقع الإسرائيلية.

1 - Cyber-Terrorist / جابر

السعودي "Cyber-Terrorist" من أشهر وأقوى الهاكرز العرب، وقد لقب بقاهر اليهود لاختراقه العديد من المواقع العالمية المتخصصة بالأمن والحماية وأنظمة الكمبيوتر مثل مايكروسوفت وكاسبر، كما نجح في اختراق مواقع العديد من البنوك والشركات الكبرى بالإضافة إلى موقع الرسام الدنمركي الذي أساء للرسول صلى الله عليه وسلم، وقد توي في نتيجة أزمة ريو حادة في أبريل 2012

2 - xOmar / عمر

حقق الهاكر السعودي عمر، والذي يعرف على الإنترنت باسم "xOmar0"، شهرة عالمية بعدما تمكن من كشف بيانات بطاقات الائتمان



الخاصة بالآلاف الإسرائيليين ما تسبب في هلع داخل الكيان الصهيوني خاصة بعدما عثرته البنوك الإسرائيلية بحدوث الاختراق لبيانات 400 ألف عميل، وقد فشلت محاولات الكشف عن هويته ما دفع داني إيلون - نائب وزير خارجية إسرائيل - إلى اعتبار الأمر إرهاب تكنولوجي متوعداً بالرد، فقام "xOmar0" بتعطيل موقع داني إيلون في هجوم استغرق نصف ساعة فقط.

3 - Sniper Hex

الهاكر السعودي "Sniper Hex" نجح في اختراق العديد من المواقع الإسرائيلية الرسمية مثل وزارة التعليم الإسرائيلية، ووزارة السياحة، ووزارة الشؤون الدينية، وموقع حزب الليكود وتدمير أكبر موقع بحث إسرائيلي "Guide" والعديد من المواقع الأخرى، ويقول "Sniper Hex" إنه تلقى العديد من العروض المالية لمساعدة أشخاص على التجسس أو اختراق حسابات شخصية لكنه رفض، مضيفاً أنه يعمل على إيجاد الثغرات الأمنية لدى المواقع العربية وتبني المسؤولين عنها وتدمير المواقع العربية الإباحية أو المواقع الغربية التي تهاجم الإسلام والعرب.

4 - كادير 11000

يطارده الهاكر الجزائري "كادير 11000" من قبل العدالة في الولايات المتحدة وفرنسا وإسرائيل وذلك نتيجة اختراقه العديد من المواقع في تلك الدول، ووفقاً لما ذكره كادير لصحيفة الشروق الجزائرية فقد اخترق أكثر من 50 ألف موقع منها موقع ماري لوبان زعيمة اليمين المتطرف في فرنسا والمعادى للإسلام، وحزب كاديما الإسرائيلي، وموقع بطاقات "ViSA" الأميركية والمواقع الجنسية العربية وغيرها، ووفقاً لكادير فإنه لا يقوم بذلك بهدف التخريب وإنما بهدف أن يكون فخراً للعروبة والإسلام، مشيراً إلى أنه يعرف أن نهاية قراصنة الإنترنت هي الموت أو السجن.

5 - علوش الحربي

بدأ الهاكر السعودي الراحل علوش الحربي رحلته في عالم القرصنة بعدما حصل على شهادة الكفاءة المتوسطة ثم توقف عن الدراسة، وبعد عدة سنوات





كعاطل اتجه لتعلم الكمبيوتر وتطبيقاته ليتفوق في برامج الحماية والاختراق وتبرز شهرته إبان الحملة التي قامت في العالم الإسلامي للدفاع عن الرسول صلى الله عليه وسلم حيث تمكن من تدمير 180 موقعاً ديمقياً، وقد لقي علوش مصرعه إثر حادث مروري بمحافظة حفر الباطن.

وتتعدد أقسام الهكر في العالم العربي إلى ثلاث أقسام هي :

1- المبتدئ: وهو أخطر أنواع المخترقين لأنه يريد تجربة كل ما تعلمه وغالباً ما التدمير للأجهزة.

2- الخبير: وهذا لا خوف منه لأنه يخترق الأجهزة فقط للبحث فيها و أخذ ما يعجبه منها.

3- المحترف: وهو يجمع الاثنين معا فأولا يأخذ الأشياء التي يريد من جهاز الضحية يترك الضحية .. والبعض يدمر.

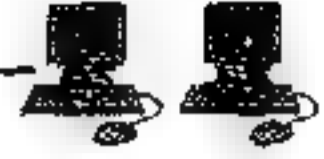
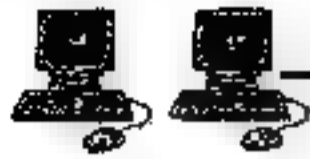
هذا وتزدحم شبكة الانترنت بالعديد من المنتديات والمواقع المتخصصة في مجال الهكر العربي . حيث أغلبها تتخصص ب إحضار الجديد في عالم الهكر من ثغرات المواقع و برامج التشفير من الحماية ودورات لاختراق المواقع و لأجهزة والبريد فضلاً عن طرق وأساليب الحماية .

المنطقة العربية سمن حرب القرصنة

تشهد المنطقة العربية وخاصة دول الخليج العربي عملية قرصنة رهيبه نابعة من حرص القراصنة على استهداف المنطقة الغنية بالنفط والتي تشهد اردهارا اقتصاديا كبيرا، ومعظم القراصنة هم من أفريقيا واروبا وروسيا ويستهدفون البنوك والحسابات الخاصة بإفراد دول الخليج بالإضافة لبعض الدول العربية.

فقد كشف تقرير مؤخر أعدته تريند مايكرو وموقع .net ITP ان المستخدمين في منطقة الشرق الأوسط يمتلكون دراية كافية بالمخاطر على الإنترنت مثل البريد التطفلي، والفيروسات والديدان الفيروسية وأحصنة طروادة، إلا أن 18





منهم فقط قد سمعوا بمصطلح «rootkits»، وهي مجموعة من الأدوات التي تُتيح للمخترقين الحصول على ميزة النفاذ إلى الأجهزة

ويتمتع القراصنة بمهارات ومعرفة عالية جداً وهم منظمون بشكل احترافي قد يصعب تتبعهم في كثير من الأوقات، ففي حين تجري عمليات القرصنة المالية للمؤسسات المالية والمصرفية العربية سواء عبر أنظمة الشبكات أو بطاقات لصراف الآلي ولكنه يحدث تتكتم شديد عليها مثلما تقتصر المجتمعات الشرقية على جرائم الشرف المنتشرة فيها.

ويقدر بعض الخبراء أن البنوك العربية تتكبد خسائر تصل إلى مليار دولار في السنة وهي في ازدياد مستمر بسبب عدم الاهتمام بأمن المعلومات الذي يأتي متأخراً لديها .

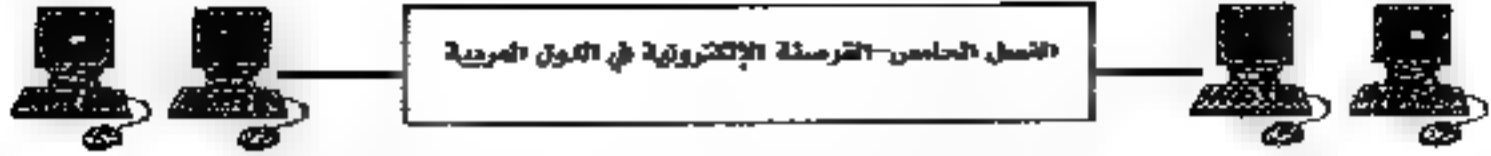
وتأتي عمليات القرصنة لديها نتيجة الاستخدام السيئ لأجهزة العمل أو شراء أنظمة أمن معلومات بأقل التكاليف بالإضافة إلى القرصنة الناتجة عن موظفين يتم إساءة معاملاتهم واحتقارهم من قبل رؤسائهم وتبرز مشكلة أخرى هي القرصنة عبر الإنترنت نتيجة استخدام بيانات البطاقات الآلية أو نشر بيانات عبر الشبكة وأجهزة الحاسوب من قبل الأشخاص أنفسهم.

إن مستقبل التجارة الإلكترونية والحكومات الإلكترونية تواجهها الكثير من التحديات، منها حجم الإنفاق على تأمين المعلومات التي لا يزيد على 5 % فقط من المبالغ المرصودة لمشروعات تكنولوجيا المعلومات العربية بينما تصل هذه النسبة إلى 35 % في معظم الدول الأوروبية.

وتشير بعض الدراسات إلى أن الخسائر المالية التي سيتعرض لها لعالم من جراء الجرائم الإلكترونية مرشحة للوصول إلى 20 مليار دولار خلال السنوات الثلاث المقبلة

ويتوقع أن يكون نصيب الدول العربية منها قرابة مليار دولار وتشكل المنطقة العربية أكثر المناطق التي يتم التركيز عليها سواء من ناحية القرصنة المالية أو التحسس وانتهاك الخصوصية وهو ما يتطلب التركيز على أمن المعلومات من





خلال زيادة الاستثمار فيها وتأهيل الكوادر البشرية في المؤسسات لمواجهة هذا الإخطبوط البرامجي من قبل قراصنة المعلومات ومتجسسي الوكالات

أسباب زيادة القرصنة الوطن العربي

تتنوع أسباب انتشار القرصنة في الوطن العربي، ويرجع الباحثون العوامل المؤدية إلى:-

1 - زيادة قاعدة مستخدمي الإنترنت في الوطن العربي

مع انتشار خدمات الإنترنت وانخفاض تكلفة الاشتراكات، بدأت قاعدة المستخدمين في الزيادة بشكل ملحوظ مقارنة بدول العالم الأخرى وهذا العدد الكبير جداً من المستخدمين للإنترنت في المنطقة، جعل الإنترنت أكثر شعبية، ووسيلة مريحة للاتصال، كما أنها فتحت أبواباً جديدة للأعمال على الإنترنت، ففي مصر بلغ عدد مستخدمي الإنترنت 11.48 مليون مستخدم، إلا أن إساءة الاستخدام زاد أيضاً؛ بسبب عدم وجود برامج توعية، لذا فقد أصبح الكثيرون من مستخدمي الإنترنت في المنطقة ضحايا للاختراقات والجريمة الإلكترونية.

2 - مشكلة البطالة

مشكلة البطالة من المشكلات التي يعاني منها الشباب وأغلبهم من خريجي الجامعات الذين يتمتعون ولو بقدر ضئيل من أساسيات استخدام الكمبيوتر والإنترنت، وإذا لم يكن لديهم إنترنت في المنزل فهم يلجئون إلى مقاهي الإنترنت، والتي تنتشر بشكل كبير في كل دول المنطقة وكل هذه العوامل تتكاتف بشكل ملحوظ؛ لزيادة الجريمة الإلكترونية، وظهور ما يسمى بمجرمي الإنترنت المحليين؛ أي من داخل المنطقة نفسها وليس من خارجها، وهؤلاء يمثلون الخطر الأكبر لديهم الوقت الكبير، ومنهم من لديه الدافع الديني، ومنهم من يعمل للدافع المادي، خاصة مع انتشار المواقع العربية التي تقدم خدمات تعليم الاختراق



3 - ضعف القوانين الرادعة

بعض البلاد العربية ليس لديها قوانين متخصصة في الجريمة الإلكترونية، والقليل من البلدان تحاول سن تشريعات لهذا النوع من الجرائم، إلا أنها ما زالت في مراحلها الأولى، وتحتاج إلى المزيد من التحسينات والتفقيح، وبسبب المشكلات السياسية في المنطقة فإن معظم الدول تلجأ إلى استخدام ما يعرف بقوانين الطوارئ Emergency Laws، عوضاً عن قوانين متخصصة للجريمة الإلكترونية. كأسلوب من أساليب الردع للجريمة الإلكترونية، على سبيل المثال: القبض على المدّونين بتهمة السب والقذف وغيرهما .

4 - القصور في برامج التوعية الأمنية

برامج التوعية بأمن المعلومات من أكثر الطرق فعالية في محاربة الجريمة الإلكترونية، فهناك نقص شديد جداً في برامج التوعية بأمن المعلومات على مستوى الأفراد والمؤسسات والحكومات.

وقد يستغل المجرمون عوامل قلة فعالية برامج التوعية بأمن المعلومات المتاحة في ارتكاب مثل هذه الحرائم، خصوصاً وأن هذه البرامج متوفرة باللغة الإنجليزية، لذا فإن هناك حاجة إلى برامج توعية وتدريب قوية تستهدف الناطقين باللغة العربية لتدريب المستخدمين، و العاملين في الشركات، ورجال القانون، لفهم المشكلة وتداركها سريعاً.

من الضروري زيادة الإرشاد والتوعية حول أمن المعلومات فهو أمر لا مفر منه لمكافحة الجريمة الإلكترونية. ففي الشرق الأوسط هناك نقص كبير في الوعي الأمني سواء بين المؤسسات أو المنظمات أو بين عامة الناس مقارنة بأوروبا.

هيننا نجد أن الدول العربية جهودها في رفع مستوى الوعي بين الناس قليلة فعلى سبيل المثال نجد أن المملكة العربية السعودية تعتبر من الدول المستهدفة لمرتكبي الجريمة الإلكترونية حيث أنها تحتل المرتبة الأولى في الشرق الأوسط و تحتل المرتبة الثامنة والثلاثون على العالم.





5- ضعف الوازع الديني و الفهم الخاطئ لبعض أمور الدين

كما قد يقدم بعض الأفراد على ارتكاب مثل هذه الجرائم بسبب ضعف الوازع الديني، و الذي يجعلهم يقدمون على بعض الجرائم بغرض الكسب المادي بغض النظر عن مشروعيته و مطابقتها للدين و مبادئه .

كما تستغل بعض المواقع الدافع الجهادي باسم الدين، و يترامن ذلك مع وجود بعض المشكلات السياسية والاقتصادية على الصعيدين العربي و الإسلامي، التي تؤدي إلى زيادة الترويج لهذه المواقع .

و هو ما أدى إلى ظهور ما يعرف بالجهاد الإلكتروني، Jihad Online، والذي تتعدد مواقعه على شبكة الانترنت. فقد تعلن بعض الجهات أنهم يستخدمون تقنيات الاختراق لمهاجمة الأعداء، و يستخدم مواقعهم وكالة فعالة للدعاية لأفعالهم، وأيضا استقطاب آخرين للمساندة والاشتراك، وأيضا تستخدم المواقع في جمع التبرعات باسم الجهاد، وأيضا الحصول على معلومات من المستخدمين والأعضاء، وقد تستقطبهم للعمل معهم، ودائما يبحث أصحاب هذه المواقع عن المواهب الشابة التي تساعد في إدارة الموقع واستخدام التقنيات الحديثة، ويتم استقطابهم بداية باسم الوازع الديني، والذي ربما يتحول فيما بعد بأساليب مختلفة إلى دافع إرهابي.

وليس بالطبع كل ما هو ديني هو إرهابي؛ ولكن نظراً لوجود الوازع الديني فإن استقطابهم من قبل هذه المواقع وتغيير أفكارهم باسم الدين لهو من الأعمال السهلة، وقد تستخدم هذه المواقع للتعرف على كيفية صنع القنابل والمتفجرات؛ وكذلك الإعداد والتخطيط للهجمات التي تحدث في أرض الواقع، وقد يستخدمون أساليب تشهير متطورة لإخفاء المعلومات عن بعض الجهات التي تراقب المواقع

6 - عدم وجود برامج للتوعية الأمنية

يرجع السبب بازدياد ضحايا الجرائم الحاسوبية لعدم وجود برامج توعية لمستخدمي شبكة الإنترنت .





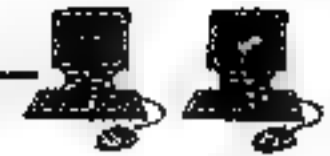
ويؤكد الخبراء الاقتصاديون أن المنطقة العربية ستتعرض إلى أزمة خطيرة في الأعوام القليلة القادمة بسبب الإحجام عن استخدام الشبكات لتفعيل التجارة الإلكترونية بين الدول العربية والأوروبية المتقدمة..

هذا الإحجام لم يكن وليد الصدفة فقد ساهمت الجرائم الإلكترونية وانتشار أشكائها خاصة مع تكرار ممرقات كروت الائتمان في إضفاء حالة من الرعب على المؤسسات الاقتصادية الضخمة وبدلاً من معالجة الأخطاء، اكتفى الجميع بالجلوس في أماكنهم!!

وتجدر الإشارة أن مصر كانت من أوائل الدول الحريصة على معارضة الجرائم الإلكترونية، حيث قامت وزارة الداخلية بإنشاء إدارة خاصة لمكافحة جرائم شبكات الحاسبات والنظم المعلوماتية وتختص الإدارة بالمتابعة اليومية للشبكات العاملة لضبط الحالات الخارجة عن القانون.. وحسبما أكد المسئولون أن الإجراءات تتخذ فوراً تجاه المخالفين ويتم تدمير المواقع إذا ثبت إضرارها بمصلحة الأمن القومي أو الآداب العامة .

وعن طرق الوقاية ومكافحة الجريمة الإلكترونية يقول سعيد على مداح خبير الحاسبات ونظم المعلومات بمعهد التخطيط القومي: لا شك أن الجرائم المتعلقة بالشبكات الإلكترونية عندما ترتبط بالجريمة المنظمة يمكن من الصعب مواجهتها لذلك للقضاء عليها لابد من إعطاء الحماية للمعلومات الشخصية عند معالجة البيانات الإلكترونية وفقاً للمبادئ التي حددتها معاهدة المجلس الأوروبي في 28 يناير 1981 مع ضرورة تطبيق برامج أكثر تشدداً ضد غسيل الأموال لتحقيق شفافية أكبر في الأنشطة المالية الدولية. كذلك لابد من التقارب بين قوانين الدول المعنية بإصدار التشريعات الرادعة في هذا المجال مع ضمان تعاون أفضل بين الهيئات القضائية وأجهزة الشرطة.





الحماية الفكرية للبرامج

تنتشر مشكلة القرصنة الإلكترونية بمعدلات مخيفة في الدول المتقدمة نظراً لارتفاع تعاملاتهم مع شبكات المعلومات بالإضافة إلى التوسع في استخدام التجارة الإلكترونية..

أما الوطن العربي فالمشكلة فيه لم تصل إلى الذروة خصوصاً وأن معظم الحالات التي تم ضبطها فردية ومع هذا لم نستطع القول إن أنظمتنا آمنة، فبالعلم بكل يوم في تقدم وهذا التقدم يحتاج إلى تطوير الآليات وتجديد البرامج التكنولوجية لمواجهة المخاطر واحتمالاتها.

إلا أن المشكلة الأساسية التي تواجه المجتمعات العربية وتقدمها هي أزمة الثقة ولتفاذي حدوثها في المستقبل ينبغي علينا الآن الاهتمام بنشر الوعي الثقافي وتدعيمه بالنظم التكنولوجية..

كذلك إعداد برامج لتأمين الشبكات وتجدر الإشارة أن بعض الشركات العربية نجحت في الفترة الأخيرة من إعداد برامج متقدمة في نظم التأمين.. أما الجانب الأكبر فيقع على عاتق القانون، فقد بات واضحاً أمام الجميع أهمية من عدد من القوانين لتقنين عمليات التحايل وذلك بالسجن أو بالغرامة.

يؤكد خبراء متخصصون في مجال البرمجيات أن إحصاءات العام الماضي سجلت انخفاضاً ملحوظاً في هذا النوع من الجرائم ويرجع الأصل في ذلك إلى النجاح الذي حققته بعض الشركات نتيجة تأمين مواقعها على الشبكة، خاصة بعد انتشار جرائم سرقة البنوك واقتحام نظم المعلومات في الشركات الكبرى والمؤسسات الحكومية ..

مع هذا فإن وسائل الاحتيايل محدودة حتى الآن في العالم العربي، لكنها تصد الانتشار خلال المرحلة القادمة وذلك بتزايد المتعاملين على الشبكات الإلكترونية



وعلى الرغم من دخول مصر في عالم الثورة التكنولوجية، واستخدام البعض لنظام الفيزا العالمية إلا أن نقص الوعي عند مستخدمي هذه البطاقات يعرضهم لكثير من المشكلات وبالتالي نحن في حاجة ماسة إلى تحديث نظم كروت وبطاقات الائتمان.

وعلى الجانب الآخر والكلام لا يزال على لسان صاحبه "سامح منتصر" هن الظروف التي يعانيها العالم العربي تضع المسؤولية على هؤلاء الشباب لتفجير إمكانياتهم وتطويرها لمواجهة الفوز الأمريكي والأوروبي لمجتمعاتنا ويؤكد الدكتور "خليل حسن" رئيس شعبة الحاسبات بالغرفة التجارية أن أشكال الجرائم الإلكترونية متعددة .. إلا أن أكثرها انتشاراً هي الجرائم الأخلاقية حيث تسببت مواقع "الشاتنج" في ارتفاع حالات الطلاق بالإضافة إلى ترويج بعض الشباب لعبارات تحمل معاني مافية للأداب العامة. ويتطابق الحال نفسه على جرائم اقتحام شبكات البنوك والشركات الكبرى والتي تسببت إلى إحداث خسائر عديدة لأصحابها.

ترتيب الدول العربية في قرصنة البرمجيات العالمية

أشارت دراسة أجرتها المؤسسة الدولية للتخطيط والبحوث (أي بي آر) أن 6 دول عربية دخلت في قائمة أعلى 25 دولة في العالم في مجال قرصنة البرمجيات مقارنة بـ 7 دول عربية عام 1999 تتراوح نسبة القرصنة فيها بين 71 في المائة و 83 في المائة مقارنة بـ 75 في المائة و 88 في المائة عام 1999. وقد تصدرت فيتنام القائمة كأعلى دولة في لقرصنة عالمياً 97 في المائة، تليها الصين 94 في المائة وإندونيسيا 89 في المائة وأوكرانيا 89 في المائة وروسيا 88 في المائة عام 2000 وكانت هذه الدول نفسها الأعلى في القرصنة عام 1999. تجدر الإشارة إلى أن الدول العربية شهدت تحسناً في درجة السيطرة على القرصنة، انعكس في خروج مصر من قائمة الـ 25 إذ تراجع نسبة القرصنة فيها من 75 في المائة عام 1999 إلى 56 في المائة عام 2000 فيما شهدت دول عربية





أخرى تحسباً ملحوظاً في مكافحة القرصنة: لبنان من 88 في المائة إلى 83 في المائة، والبحرين من في المائة إلى 80 في المائة، والكويت من 81 في المائة إلى 80 في المائة، وسلطنة عمان من 88 في المائة إلى 78 في المائة والأردن من 75 في المائة إلى 71 في المائة فيما ارتفعت النسبة قليلاً في قطر من 80 في المائة إلى 81 في المائة.

وأشارت الدراسة إلى أن من أبرز الأسباب التي أدت إلى ذلك وجود فجوة بين عدد أجهزة الحاسوب المستخدمة وبين البرامج المتوافرة لتشغيل هذه الأجهزة، فظي مطلع التسعينات فتحت أسواق الحاسوب خارج الولايات المتحدة الأميركية، وانتشرت الأجهزة في دول العالم دون أن يكون هناك انتشار واسع للشركات المنتجة للبرامج لذلك اضطر مستخدمو الأجهزة إلى استخدام البرامج المقرصنة مع عدم وجود وكلاء مفوضين من شركات البرمجيات وهو أمر بدأت الشركات في استدراكه ومعالجته بالإضافة إلى تعزيز وجود الشركات المنتجة للبرامج على الساحة الدولية، مما أتاح للمستخدمين شراء البرامج الأصلية، واثاح هذا الوجود زيادة في الدعم الفني الذي تقدمه للبرامج التي تنتجها، مما شجع المستخدم على شراء النسخة الأصلية علاوة على الهبوط الكبير لأسعار هذه البرامج مقارنة بعامي 1996 و 1997، مما أدى إلى تصغير الفجوة بين البرامج الأصلية وتلك المنسوخة بطريقة غير شرعية.

ومن الأسباب الأخرى قيام شركات مناهضة للقرصنة مثل بيزنس سوفتوير اللانيس وسوفتوير اند انفورميشن اندستري اسوسييشن بحملات توعية لأهمية الملكية الفكرية والترويج لشراء النسخ الأصلية بالإضافة إلى دخول الشركات التي تهتم باستخدام برامج بصفة غير شرعية في الأسواق العالمية في صراعات جانبية أثرت في مجال عملها المباشر، وتزايد تعاون الحكومات لإيجاد نظم تشريعية لحماية الملكية الفكرية ولوضع عقوبات تجريبية لقرصنة البرامج.

وأوضحت الدراسة إلى إمكانية أن يكون هذا التراجع في نسبة القرصنة قد اقترب من نهايته، فعام 2000 تميز بنمو بطيء نسبياً كما أن القرصنة حافظت على ثباتها بشكل عام. ويبدو أن هناك تغيراً في السلوك والتصرف بين الفترات التي يكون فيها نمو اقتصادي جيد، حيث تقوم الشركات بإدخال تكنولوجيا جديدة





للمحافظة على الطلب والمحافظة على التنافس في أوجه، وبين الفترات التي يكون فيها نمو الاقتصاد بطيئاً.

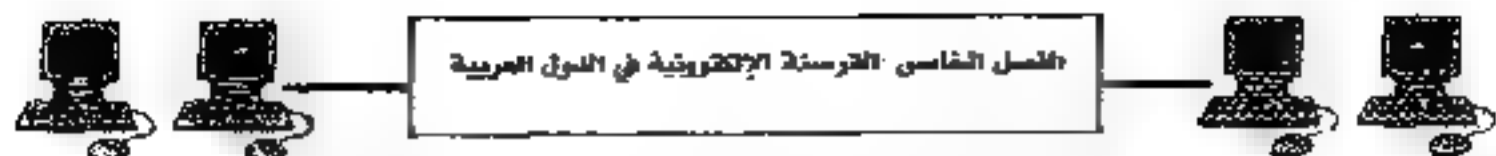
كما أن هذه النتائج تشير إلى وجود مشكلة كبيرة متعلقة بالقرصنة في الدول التي تعتبر دولاً متقدمة في مجال التكنولوجيا، خصوصاً أميركا الشمالية وأوروبا الغربية، إذ أظهرت هذه الدول انخفاضاً متواضعاً في نسبة القرصنة أو حافظت على نسبتها أو ارتفعت نسبة القرصنة فيها، وعلى الرغم من أن هذه الدول لديها أقل نسبة للقرصنة في العالم، إلا أنها تظهر تقدماً أقل في خفض القرصنة، صكماً أن الدول التي نما اقتصادها بشكل كبير خلال العام هي الدول التي لديها أعلى نسب قرصنة وخاصة دول منطقة آسيا والباسفيك التي وصلت قيمة الخسارة فيها إلى 4 مليارات دولار لأول مرة مما جعلها أعلى منطقة خسارة في مجال البرمجيات عام 2000، فيما احتلت أوروبا الغربية المرتبة الثانية، واحتلت أميركا الشمالية المرتبة الثالثة وتراجعت نسبة القرصنة في دول الشرق الأوسط وأفريقيا بشكل واضح، ويوضح الجدول التالي الخسارة الناتجة عن القرصنة في مناطق العالم المختلفة بالترتيب التنازلي الذي يعكس أعلى منطقة في القرصنة إلى أدناها ما بين عامي 1999 و2000.

الهاكرز العرب والمواقع الإسرائيلية

وسع القراصنة العرب هجماتهم على المواقع الإسرائيلية الهامة حيث قام القراصنة باحتراق وإسقاط أكثر من موقع إسرائيلي ومنها اثنان من أكبر المستشفيات الإسرائيلية وشركة المواصلات العام "دان" وموقع "فيستيفال" بالإضافة إلى موقع صحيفة "هيرتز" الإسرائيلية.

ووجد كل من دخل على موقع "فيستيفال" الإسرائيلي رسالة من القراصنة العرب تقول الحرية لفلسطين والموت لإسرائيل كما وجد المتصفّحون للمواقع الأخرى رسالة تقول أن هناك أربعة إسرائيليين سيواجهون مصير جلعاد شاليط.





وبدأ الهجوم عندما استهدف القراصنة العرب، موقعا مركزين طبيين في وسط المدينة وهما "تيل هاشومر" و "مركز أسوتا الطبي".

ويدعي مسئولان من المراكز الطبية التي هوجمت أن الهجمات لم تلحق الضرر بالمواقع الالكترونية التابعة لهم وأن نظام آلية الحماية الالكترونية استطاع التصدي للهجمات وأن ملفات المرضى كما هي ولم يلحق بها أي ضرر، وهذا بالطبع مخالف لما وصفه كل من حاول الدخول إلى الموقع.

احتفل مجموعة من الهاكرز المصريين بذكرى نصر أكتوبر على طريقتهم الخاصة، وذلك باختراق عدد من "السيرفرات" التي تخدم مواقع صهيونية، ووضع علم مصر على الصفحة الرئيسية.

وأعلن فريق "الهاكرز المصريين" team haker egypt في ساعة مبكرة من صباح اليوم السبت، أنه اخترق سيرفرين خاصين بشركة "لايت سبيد" الداعمة للمواقع الصهيونية والهولندية، وقام بوضع صورة رفع العلم المصري على أرض سيناء، وصور الأسرى الصهاينة.

كما وضع فريق الهاكرز رسالة باللغة العبرية على الصفحات الرئيسية للسيرفرات تقول "سوف تعيش مصر حرة مستقلة إلى الأبد، واليوم نحتفل بنصر أكتوبر العظيم، وسوف نفسدهم عليكم.. تحيات الشعب المصري".

وأكد الهاكرز أنهم عازمون على استكمال عملية اختراق المواقع الصهيونية، طوال اليوم وحتى منتصف الليل، وذلك تعبيرا عن موقفهم من الكيان الصهيوني، وفقا لبوابة الأهرام.

وكان الفريق ذاته، قد قام الأيام الماضية، باختراق مواقع استضافة إيرانية تضامنا مع الشعب السوري واحتجاجا على موقف طهران الداعم لنظام الأسد ضد الثورة السورية.

ويحتفل الشعب المصري والشعوب العربية والإسلامية عامة، بالذكرى التاسعة والثلاثين لنصر أكتوبر 1973/ رمضان 1393، وهي آخر حرب يخوضها الجيش المصري، نجح خلالها في اقتحام وعبور قناة السويس، وخط بارليف.



الحصين، وهي الحرب التي شاركت فيها الكثير من الدول العربية والإسلامية، من خلال دعم الجيش المصري ومنع النفط عن الدول الغربية وعلى رأسها الولايات المتحدة

وكان موقع (فضايا مركزية) الإسرائيلي الإخباري قد نقل في وقت سابق على الشبكة العنكبوتية، عن رئيس جهاز الأمن العام (الشاباك) السابق، يوفال ديسكين، تحذيره من الأخطار الكبيرة التي قد يلحقها قراصنة الحاسوب العرب بالدولة العبرية، معتبرا أن ما يحدث اليوم قد ينذر بما أسماها بالحرب الإرهابية الواسعة على إسرائيل، ووسائل الحماية والجهود المبذولة اليوم لا ترتقي لحجم ما قد تواجهه إسرائيل في المستقبل، على حد تعبيره.

وزاد الموقع قائلاً إن تصريحات ديسكين وردت في ختام مؤتمر عقد في فندق هيلتون بإسرائيل، بمشاركة دولية .

مشيرا إلى أنه يوجد اليوم الملايين من أجهزة الحاسوب في العالم والمرتبطة بشبكة الانترنت، وإلى جانبها ملايين من الأجهزة الخليوية الذكية، والتي يستطيع قراصنة الحاسوب (هاكرز) من خلالها الدخول والقيام بالعديد من العمليات دون رقابة.

وأضاف ديسكين أن هؤلاء الهاكرز يستطيعون السيطرة على مدن كاملة وقطع الكهرباء عنها، والتسبب بأضرار كبيرة وواسعة للعديد من المصانع، والعديد من الأضرار الأخرى، والتي تعتبر حربا إرهابية شاملة على إسرائيل، على حد وصفه. وتزامنت تصريحات ديسكين مع نشر التقرير الأمني الإسرائيلي الجديد الذي أشار إلى أن إسرائيل والسويد وهولندا من أكثر دول العالم المستعدة لمواجهة حالات القرصنة الإلكترونية، كما احتلت بريطانيا وأمريكا وإسبانيا وفرنسا وألمانيا مركز متقدمة بين الدول الناجحة في مواجهة الهاكرز.

وقد أجريت الدراسة بالتعاون مع شركة (مكا) الناشطة في مجال الحماية من القرصنة في الإنترنت، التي صنفت دولاً كالبرازيل والمكسيك والصين ضمن الدول الأقل نجاحاً في حماية فضائها الإلكتروني. وشدد معدو التقرير،





بحسب صحيفة 'هآرتس' على أهمية التنسيق والتعاون بين دول العالم لتعريب الحماية ومواجهة القرصنة قبل نجاحهم بتنفيذ هجماتهم.

كما اقترحوا اعتماد قوانين صارمة لإزاء مرتكبي الجرائم الإلكترونية العابرة للحدود. وبحسب اختصاصي إسرائيلي كبير في التكنولوجيا فإن موضوعية التقرير هي أكبر قوة له، وما يقدمه التقرير هو إدراك الخبراء لمدى التأهب الأمني، والعمل في مجال الأمن الإلكتروني بشكل مستمر.

ويؤكد التقرير على أن السويد وإسرائيل وفنلندا أبهرت المختصين بالإجراءات المتخذة لحماية الإنترنت، خاصة إسرائيل التي تتعرض لـ 1000 عدوان إلكتروني في الدقيقة الواحدة.

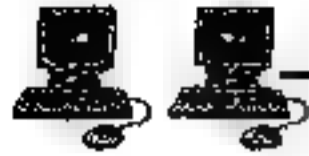
واقترح التقرير ما قاله كبير مستشاري رئيس الوزراء الإسرائيلي لشؤون الأمن الجنرال في الاحتياط، يتسحاق بن إسرائيل بأن مجموعة الهاكرز المعروفة باسم أنونيموس، وتعني بالانكليزية مجهول، تقوم بشن كثير من الهجمات، لكنهم لا يسببون الكثير من الضرر، مشيراً إلى أن التهديد الحقيقي هو من الدول ومنظمات الجريمة الكبيرة.

كما طمأن المستشار الإسرائيليين مؤكداً على أن الدولة العبرية تمكنت من تكوين قوة إلكترونية تقيم التهديدات المتعلقة بالبنية التحتية الرئيسة كمرفق إنتاج الكهرباء وإمدادات المياه وتنمدي لها، على حد تعبيره.

وكشف بن إسرائيل، وهو أيضاً المسؤول عن لجنة مكافحة الهجمات الإلكترونية، للإذاعة الإسرائيلية أمس، عن وجود هيئة خاصة مسؤولة عن حماية البيانات، تعمل منذ الأول من كانون الأول (ديسمبر) الماضي، لكنه أكد في المقابل أن هذا لا يعني أن بإمكاننا في غضون أسبوعين، أن نجد حلولاً للمشاكل، إذ سيستغرق ذلك ما بين عام أو عامين، قبل أن نتمكن من صد هجمات القرصنة من كل أنحاء العالم.

وأضاف أن المواقع التابعة للجيش والاستخبارات جرت حمايتها كأولوية، وتحديدًا منذ خمسة عشر عاماً.





وخلص الوزير الإسرائيلي إلى القول إن هدف هجمات السائبر ليس الإضرار بالمواقع الإلكترونية الإسرائيلية، بل إرباك منظومات حساسة في إسرائيل، إضافة إلى سرقة معلومات سرية والتسبب بإحداث خلل في هذه المنظومات المرتبطة بالأنظمة المحوسبة، على حد قوله.

القرصنة الإلكترونية في الاردن

لعبت «مايكروسوفت» أدواراً مهمة في تطوير قطاع تكنولوجيا المعلومات في الاردن والقطاعات الأخرى المرتبطة.

ويبدو أن اهتمام «مايكروسوفت» بالاردن والسوق الاردنية يتجاوز الاهتمام والعمليات التجارية للشركة العالمية، وتتمثل بالاتفاقية الاستراتيجية الموقعة مع الحكومة الاردنية والتي تشمل المساهمة في تطوير القطاع والموارد البشرية الاردنية والمساهمة في تطوير قطاعات أخرى على رأسها القطاع التعليمي.

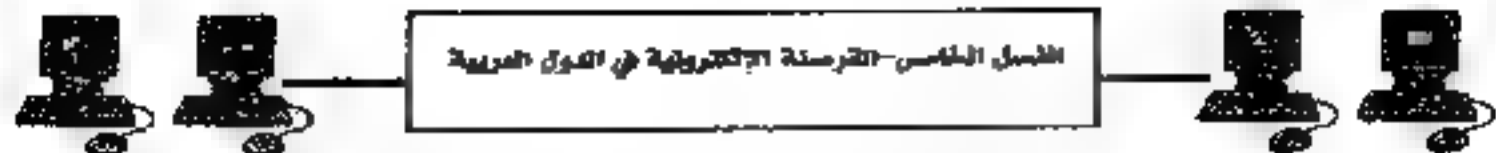
وتنظر «مايكروسوفت» الى تواجد طويل الأمد في المملكة، فضلاً عن اهتمامها في تجديد وتطوير هذا التواجد من خلال تجديد الاتفاقية الاستراتيجية مع الحكومة الاردنية.

كما أن تواجد الشركة في المملكة لا يقتصر على الاتفاقية مع الحكومة فهي تمتلك رصيداً كبيراً من الشراكات في مختلف القطاعات الاقتصادية وهي تسعى لتطويره على الدوام، مثل الاتصالات، والبنوك، والشركات الصغيرة والمتوسطة، بالإضافة الى اهتمامها بتطوير القطاع التعليمي والاهتمام بالشباب الرياديين والمطورين.

وتعتبر محاربة ظاهرة القرصنة في الاردن وغيرها من دول العالم جزءاً أساسياً في حل المشاكل الاقتصادية المرتبطة بقطاع تكنولوجيا المعلومات والقطاعات الاقتصادية الأخرى.

و تخسر مايكروسوفت عالمياً كل عام مليارات الدولارات بسبب القرصنة خاصة في ظل تنامي القرصنة في الأسواق الناشئة.





قطع الأردن شوطاً كبيراً في محاربة القرصنة ويتضح ذلك من خلال تراجع نسب القرصنة، فعلى مدى السنوات من 2007 الى 2010 انخفضت نسبة القرصنة في المملكة بنسبة 3% لتصل الى 57% لتكون هذه النسبة في الأردن ولأول مرة أقل من المعدل الاقليمي البالغ 58%.

من جهة أخرى ان تقنية الحوسبة السحابية تستحوذ اليوم على اهتمام الشركة العالمية في تسويق خدماتها ومنتجاتها، كما ان المنافسة العالمية في اطارها تزداد يوماً بعد يوم، كما ان هنالك تقبلاً ووعياً يزداد من سنة الى أخرى في المنطقة لتبني هذه التقنية وخدماتها ومنتجاتها المختلفة والتي تهدف الى توفير التكاليف بشكل كبير على المنشآت الاقتصادية والمساهمة في تطوير القطاعات الاقتصادية بكافة.

وحافظت المملكة على مكانتها كواحدة من افضل ثلاث دول في الشرق الاوسط على صعيد حماية الملكية الفكرية للأفراد والشركات المحلية والدولية.

وقال مدير عام دائرة المكتبة الوطنية محمد يونس العبادي ان قانون حماية الملكية الفكرية الاردني واضح وصريح في إشارة الى أن كافة البرمجيات المقرصنة وغير المرخصة هي منتجات غير قانونية في المملكة، مضيفاً الى ان تخفيض نسبة القرصنة في الأردن سيعود على الجميع بمنافع عدة، أهمها أن حماية الملكية الفكرية هي أحد أبرز عوامل النمو الاقتصادي، حيث أنها تسهم في رفع العوائد الضريبية، كما أنها تسهم في خلق فرص عمل جديدة وتحذب الاستثمارات الأجنبية للمملكة، وتحمي المبدعين والمتميزين الأردنيين.

وبحسب دراسة أطلقها اتحاد منتجي برامج الكمبيوتر التجارية هذا العام حول قرصنة البرمجيات عالمياً، فإن القيمة التجارية للبرمجيات المقرصنة حول العالم بلغت 63.4 مليار دولار في العام 2011، كما ان خفض نسبة القرصنة بـ 1 / فقط كفيل بزيادة حجم المنتج الاقتصادي العالمي بما قيمته 40 مليار دولار، وانخفاض نسب القرصنة بـ 10% عالمياً سيغني خلق 2.4 مليون فرصة عمل جديدة، وبموا



اقتصاديا بقيمة 400 مليار دولار امريكى وعوائد ضريبية بقيمة 67 مليار دولار حول العالم

فيما تراجع الاردن خلال العام الماضي بنسبة 1% في مكافحة القرصنة لتصل النسبة الى 58% مما ميزيد من القيمة التجارية للبرمجيات المقرصنة في الاردن والتي بلغت 31 مليون دولار في العام 2011.

وأشار الخبير الاقتصادي الدكتور يوسف منصور الى الآثار الاقتصادية السلبية للقرصنة على المملكة مشدداً على انعكاساتها وأضرارها الكبيرة على الافراد و لشركات وعلى تعزيز بيئة الابداع بشكل عام في المملكة.

السعودية والإمارات تتصدران دول الخليج في الجرائم الالكترونية

أكد تقرير أمن المعلومات الإلكترونية في معهد الدراسات الدبلوماسية إن السعودية والإمارات تتصدر المركزين الأول والثاني على التوالي على مستوى دول مجلس التعاون الخليجي في التعرض للجرائم الالكترونية.

مشيراً إلى حدوث أكثر من 700 ألف حالة انهيار نظامي خلال 9 اشهر في السعودية ، لافتاً إلى أن حجم القرصنة الالكترونية على المستوى العربي من عام 2008 إلى 2010 بلغ نحو مليار دولار.

وأرجع التقرير دوافع الهجوم على أنظمة المعلومات الى الانتقام او اثبات الذات او دوافع مالية مع وجود ثغرات أمنية في نظام المعلومات او البرمجيات او قواعد البيانات او أنظمة التشغيل، مما يمكن المهاجم من سرقة المعلومات ومهاجمة الشبكة الداخلية وفتح ثغرات أمنية في أنظمة الحماية.

في حين يكون المهاجمون من الخارج أقل خطراً من الهجوم الداخلي لكن يحدث ضجة اعلامية عند وقوعه ويكون له دوافع مثل التجسس والتخريب كما يمكن من خلاله تحقيق اهداف سياسية وتجارية، كما يتم استخدام الوسائل الممكنة لجمع اكبر قدر من المعلومات عن الضحية لغرض شن الهجوم كدخول مكان الضحية او الهاتف او الانترنت.





القرصنة الإلكترونية في الإمارات

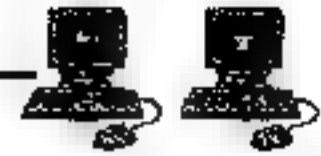
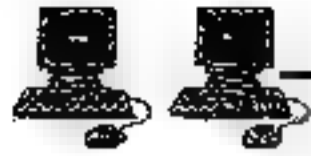
"تشير الإحصائيات العالمية إلى أن اختراق الإنترنت في منطقة الشرق الأوسط ارتفع بأكثر من 21 في المائة في يونيو/حزيران، مسجلاً زيادة في عدد مستخدميه وصلت نسبتها إلى حوالي 1177 في المائة خلال السنوات الثمانية الماضية ومؤخراً، شهدت الإمارات عدداً من عمليات القرصنة والتي حدثت بعدد كبير من البنوك إلى تشديد احتياطاتها الأمنية لحماية عملائهم. كما قامت هيئة تنظيم الاتصالات في الدولة مؤخراً بإغلاق صفحة على الإنترنت لوكالة توظيف وهمية متصلة بالصفحات الإلكترونية لوزارة العمل ووزارة التربية والتعليم وإدارة الجنسية والإقامة في دبي.

وأشار الدكتور علول إلى أن قراصنة الإنترنت يصممون صفحات على الإنترنت مطابقة لصفحات إلكترونية لشركات معروفة كبيرة، مثل: المؤسسات المالية، والبنوك، وغيرها، مع تطابق كبير في العنوان الإلكتروني لهذه المؤسسات والشركات.

ويؤكد الدكتور علول إن عمل صفحة وهمية على الإنترنت هو أمر هين، حيث يقول: "يمكن لقراصنة الإنترنت أن يشتروا عنواناً إلكترونياً مماثلاً لحد كبير للعنوان الإلكتروني للمؤسسة أو الشركة التي يريدون خداع عملائها." وأضاف: "ويقوم قراصنة الإنترنت بشراء العنوان الإلكتروني بواسطة بطاقة ائتمان مسروقة لتخلص من أي دليل يمكن أن يربطهم بالصفحة الوهمية. بعد بناء الصفحة الإلكترونية الوهمية، يقوم القراصنة بفتح رسائل إلكترونية لمستخدمي الإنترنت ثم يجلسون في انتظار معلوماتهم."

وحذر الدكتور علول من الوثوق بأية رسائل إلكترونية تطلب معلومات شخصية عن المستخدم، ونصح بتحميل برامج محاربة القرصنة التي يمكن الحصول عليها مجاناً من الإنترنت. كما حذر من وضع أية معلومات شخصية يمكن لقراصنة الإنترنت الوصول إليها في المنتديات الاجتماعية الإلكترونية على الإنترنت مثل Facebook و My Space وغيرها.





يشير التقرير إلى أن أكثر أشكال الجريمة الإلكترونية انتشاراً بالإمارات هي الفيروسات أو البرمجيات الخبيثة التي تستهدف الحواسيب بنسبة 51 بالمائة، تليها رسائل الاحتيال الإلكترونية بنسبة 19 بالمائة، ثم هجمات تصيد المعلومات الخاصة والسرية بنسبة 18 بالمائة.

وتعتمد أنشطة الجريمة الإلكترونية على رسائل الاحتيال الإلكترونية وهجمات تصيد المعلومات الخاصة والسرية لسرقة المعلومات المصرفية وبيانات البطاقات الائتمانية لاستغلالها في أغراض إجرامية.

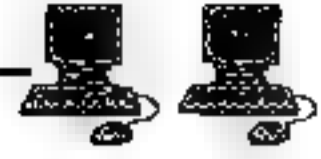
كما حذر خبراء "نورتن" من أنشطة الجريمة الإلكترونية التي تستهدف الأجهزة الجواله إذ أشار التقرير إلى أن قرابة 20 بالمائة من كافة أنشطة الجريمة الإلكترونية بالإمارات تستهدف الأجهزة الجواله، في ظل اعتماد قرابة 56 بالمائة من مستخدمي الهواتف الجواله للتنفاذ إلى الإنترنت.

وتحتل الامارات عربياً الـ 12 على التوالي في مجال حماية الملكية الفكرية ومكافحة أعمال القرصنة، فيما تبذل الجهات المعنية جهوداً مكثفة في حماية حقوق الملكية الفكرية ومنع الانتهاكات والاعتداءات الإلكترونية.

وصنفت ضمن أفضل 22 دولة عالمياً في هذا الإطار، حيث أسست محكمة متخصصة بالجرائم الإلكترونية في العاصمة أبوظبي، وجهاز لمواجهة أعمال القرصنة الإلكترونية في دبي متمثل في شرطة الجرائم الإلكترونية، إضافة إلى العديد من الجهات الأخرى ذات الاختصاص في بعض الدوائر المحلية.

ويأتي ذلك في وقت تشهد فيه المنطقة العربية بشكل عام نمواً لافتاً في أعداد مستخدمي المواقع الاجتماعية وشبكات التواصل، بصورة تزيد من الأعباء الملقاة على عاتق الجهات الرسمية في هذه البلاد، خصوصاً في عمليات التصدي لأنواع متطورة من الهجمات الإلكترونية، فطالما يجري المراسنة الإلكترونيون تحديثاً على أنظمة الاختراق لتتناسب مع الأنظمة الأمنية الجديدة الموضوعة من قبل السلطات المعنية.





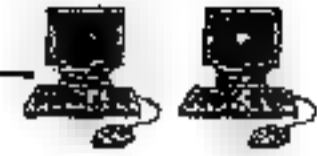
ولفتت نسبة تعرض المحتوى الرقمي للقرصنة في الإمارات تصل إلى 36 بالمئة، حسب دراسات وأبحاث عالمية، في حين تستطيع الدولة توفير نحو 939 فرصة عمل وإضافة 1.7 مليار درهم (456 مليون دولار) إلى الناتج المحلي الإجمالي في حال قامت بتخفيض القرصنة بنسبة 10 بالمئة إضافية خلال الأعوام العشرة المقبلة. وتقوم الجهود الحكومية المكثمة بخطى سريعة الإيقاع في الصترة الأخيرة، والتي تمثلت في تأسيس محكمة متخصصة بالجرائم الإلكترونية في أبوظبي ومن بينها عمليات القرصنة، وجهاز لمواجهة القرصنة الإلكترونية في دبي (شركة الجرائم الإلكترونية)، فضلاً عن الأجهزة المتخصصة التابعة للبنوك والمؤسسات المالية الكبرى، التي تعمل على رصد عمليات التزوير والتحايل على الأجهزة الإلكترونية، وبالصورة التي حدث بشكل كبير من عمليات النصب والاحتيال الإلكترونيين.

وكان خبراء وعاملون في قطاع تكنولوجيا المعلومات، قدروا خسائر الإمارات جراء عمليات القرصنة والاحتيال الإلكتروني خلال العام الماضي بنحو 200 مليون درهم (نحو 55 مليون دولار)، بما يعادل 33 بالمئة من إجمالي حجم الجرائم الإلكترونية على مستوى منطقة الخليج العربي عموماً، والتي تقدر بنحو 600 مليون درهم (163 مليون دولار)، معتبرين أن وجود شركات صغيرة ومتوسطة تنافس في الأسواق دون الانتباه إلى أهمية التحوط لهذه العمليات، أو حتى رصد ميزانيات سنوية لها، من شأنه أن يرفع من مخاطر الهجمات الإلكترونية على قطاع الأعمال.

القرصنة الإلكترونية في السعودية

لا يزال هناك قلق عالمي كبير على المستوى الأمني والاقتصادي والإداري نتيجة الاختراقات الإلكترونية المتعددة التي تشهدها المنشآت مما جعل من أمن المعلومات هاجساً لدى الدول والشعوب والمنظمات والشركات والمنشآت الاقتصادية وذلك على كافة المستويات الأمنية والإدارية والاقتصادية.





وطالب خبراء اقتصاديون ومختصون في أمن المعلومات بضرورة تطبيق معايير عالمية في مجال حماية المعلومات في كافة المنشآت الوطنية خاصة البنوك والمنشآت التي يحتم عليها حفظ معلومات ضخمة سواء للأفراد أو المنشآت.

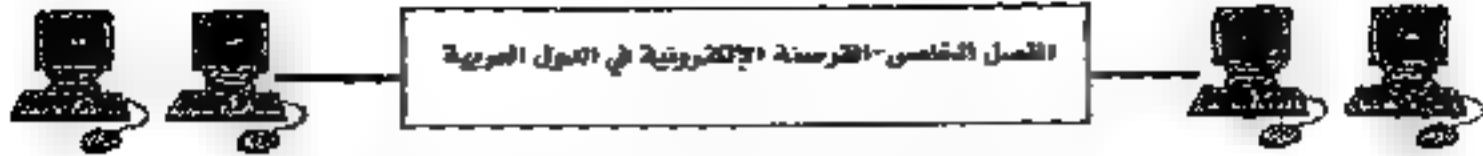
في ظل ما نطالعنا به الأخبار من فترة لأخرى لاختراقات حدثت لشبكات معلومات عالمية مهمة أو لقرصنة المعلومات من مواقع العديد من الجهات ومنها ما نشر عن قرصنة المعلومات لموقع البنتاجون مما يستدعي الاهتمام بأمن المعلومات والبحث عن الوسائل والبرامج الكفيلة بحماية معلومات منشآت الوطنية المختلفة.

وفي هذا الإطار يشير خبراء ومختصون في الامن المعلوماتي إلى أن الاختراقات والقرصنة الإلكترونية تهدد العديد من المنشآت المحلية المهمة، كما أن العديد من الحقائق المرتبطة بمجال تقنية المعلومات وسهولة الاتصالات على مستوى العالم نتج عنه العديد من الحقائق منها أن هناك ملياري مستخدم للإنترنت حول العالم وأن وسائل التواصل الاجتماعي هي النشاط الأول على شبكة الإنترنت الآن، ويأتي اهتمام معظم الشركات والمنشآت الوطنية لتطبيق مفهوم السياسات الأمنية للمعلومات وذلك لعدم وعيها بفوائد تلك السياسات التي من شأنها أن تقلل من المخاطر الأمنية التي تتعرض لها.

وعليه بات من الضروري تحفيز المنشآت الوطنية لتبني المعايير والسياسات الأمنية العالمية والتي تهتم بتأمين البيانات التي تخص المنشآت والمستفيدين منها ورفع المستوى الأمني بشكل عام في جميع تعاملات المنشآت الإلكترونية من الأمن المادي إلى الأمن الإلكتروني.

ويطالب الخبراء في هذا المجال بأهمية قيام الجهات المختلفة بتطبيق وتبني المنشآت للبرامج المساعدة في حفظ البيانات والمعلومات الخاصة بها وحمايتها من أي اختراقات أو قرصنة قد تتعرض لها حتى لا تتأثر هذه المنشآت بهذه الاختراقات والتي تساعد المتعاملين مع هذه المنشآت وتعرض في نفوسهم الثقة تجاه مثل هذه المنشآت نتيجة لاستخدامها برامج حماية لكافة تعاملاتها .





كما وتعرضت شبكة كمبيوترات شركة النفط العربية السعودية "أرامكو"، أكبر منتج للنقط في العالم، للاختراق بفيروس، يعتقد أن أحد كبار المسؤولين ممن يمكنهم الوصول إلى الشبكة ساعد المخترقين "الهاكرز" باستهداف الشبكة في أغسطس الماضي.

ويعتبر الهجوم بفيروس "شامون" Shamoon، الذي استهدف كمبيوترات أرامكو وحداً من أكثر الهجمات الفيروسية التي تستهدف شركة واحدة فقط. ويمكن للفيروس "شامون" أن ينتشر عبر شبكة الكمبيوترات الداخلية ويمسح محتويات القرص الصلب في أجهزة الكمبيوتر.

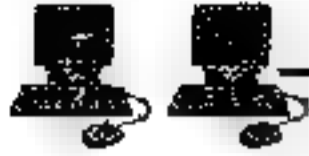
وقالت أرامكو السعودية إن الضرر الذي لحق بكمبيوتراتها كان محدوداً ومقتصرًا على كمبيوترات المكاتب، ولم يؤثر على أنظمة التشغيل التي قد تلحق الضرر بالعمليات الفنية، كما أن أنظمة التحكم وبيانات الحقول لم تتأثر بهذا الهجوم.

وأبلغ مصدر على اطلاع على التحقيقات الجنائية رويترز أن "شخصاً لديه معرفة بالداخل ومزايا داخل الشركة متورط في المسألة".

غير أن مصدراً آخر بالشركة قال في وقت لاحق تعرضت أنظمة الإلكترونيات لاختراق، وهذا الفيروس جاء فيما يبدو من خارج الشركة وليس من شخص داخل أرامكو. مازال التحقيق جارياً لمعرفة ما حدث.

وفي وقت لاحق أفادت شركة غاز قطر بتعرضها لهجوم فيروسي، ما يشير إلى احتمال تعرض شركات مماثلة في المنطقة لهجمات من هذا القبيل، رغم عدم الربط بين الحادثتين.

وقالت شركة "راس غاز" القطرية، التي تعد ثاني أكبر مصدر للغاز الطبيعي المسال في العالم، الخميس إنها اكتشفت فيروساً في شبكة أجهزة الكمبيوتر في مكاتبها.



وقالت "راس غاز"، وهي واحدة من شركتين منتجتين للغاز الطبيعي المسال في قطر، في بيان إن أجهزة الكمبيوتر في مكاتبها أصيبت بفيروس غير معروف تم اكتشافه الاثنين.

غير أنها أوضحت أن أنظمة التشغيل مؤمنة وأن الفيروس لم يؤثر على الإنتاج في منشأتها بمدينة راس لقان الصناعية أو الشحنات المقررة. وأعلنت مجموعة قرصنة كمبيوتر تطلق على نفسها اسم "سيف العدالة البتار" مسؤوليتها عن الهجوم الذي استهدف شبكة كمبيوترات "أرامكو" وقالت المجموعة إن اختراق شبكة "أرامكو" منحها حرية الوصول إلى وثائق خاصة بالشركة وهددت بالكشف عن أسرار الشركة، غير أنه لم يشر أي وثيقة من هذه الوثائق حتى الآن. وأوضحت الجماعة أن ما قامت به له بواعث "سياسية"، مشيرة في هذا الصدد إلى أن الهجوم يأتي لمواقف الرياض من سوريا والبحرين.

القرصنة الإلكترونية في الجزائر

انتشرت القرصنة الإلكترونية في الجزائر بصفة واسعة وبين مركز البحث في الإعلام العلمي والتقني "سيرست" في الجزائر أن معظم البرامج المستعملة من قبل الجزائريين هي برامج مقرصنة، ابتداء من أنظمة التشغيل منها نظام "الونداوس" ومختلف طبعاته المستعملة.

ويشير التقرير إلى أن استعمال البرامج غير المقرصنة يمد جداً ضئيل في الجزائر. ويقتصر على بعض مؤسسات الدولة والذي يبقى غير كاف لأن البرامج المقرصنة تباع في الأماكن العمومية دون حسيب أو رقيب وتقتنى بسهولة، كما أن الإقبال عليها واسع نظراً لثمنها الزهيد مقارنة بتلك الأصلية.

ويعود ذلك إلى عدم استيعاب أهمية الأمن المعلوماتي، والثغرات والعيوب التي تحتوي عليها البرامج المقرصنة والتي تهدد أمن الأنظمة المعلوماتية، بينما يجب





الذهاب نحو المصادر المجانية "open sources" المعروفة بأمنها وإمكانية معرفة ثغراتها.

وتعتبر أحسن طريقة لمواجهة القرصنة هو من سياسة وطنية لتشجيع هذه الأنظمة لحرية، ووضع مصلحة لأمن المعلومات والوقاية من الاختراقات والهجمات التي تهدد شبكات المعلوماتية الوطنية والتي تمس بوابات المواقع الجزائرية، خاصة أن ما طرأ في السنوات الأخيرة من تطور في وسائل النسخ والإنتاج الإلكتروني تجاوز الحدود، حيث تباع النسخ المقرصنة غالبا بأسعار منافسة للنسخة الأصلية.

وعلى الصعيد ذاته اعتقلت الشرطة القضائية الجزائرية شاباً من إحدى الولايات الواقعة شرق البلاد (باتنة)، وقدمته إلى المحكمة بتهمة القرصنة الإلكترونية، بعد تمكنه من اختراق موقع وزارة الدفاع الأمريكية (البنتاغون)، والقيام بتخريب محتويات بعض الملفات والوثائق السرية.

القاضي أمر بتوقيف الشاب الجزائري. إلى حين تقديم لائحة اتهام بحقه لاحقاً، بتهمة القرصنة الإلكترونية، والدخول عبر شبكة الانترنت، إلى مواقع وتدميرها والتعبث بمحتوياتها دون وجه حق.

تم إلقاء القبض على الشاب، بعد تحريات سرية للغاية، بطلب من طرف الشرطة الدولية (الإنتربول)، التي أخطرت منذ أشهر من قبل وزارة دفاع لولايات المتحدة، بأن شخصا جزائريا قام باختراق موقع الوزارة، وقام بتخريب محتوياته من وثائق ومفاتيح سرية، وأن المتهم يقوم بالدخول إلى موقع مركز البورصات المالية، ويستولي على أموال طائلة عن طريق تحويلها إلى أرصدة مجهولة الوجهة.

الأجهزة الأمنية الأمريكية قامت بالتنسيق مع أجهزة الأمن الجزائرية بعد الطلب الموجه لها من قبل (الإنتربول) وأسفرت تحريات الأجهزة الأمنية الجزائرية عن تحديد هوية الشخص المعنى الأول في الموضوع، وهو شاب من ولاية باتنة البالغ من العمر 22 عاما، وألقي القبض عليه في بيته، وتم ضبط مبالغ مالية كبيرة لديه ومن مختلف العملات، خاصة منها الدولار واليورو.





القرصنة في المغرب

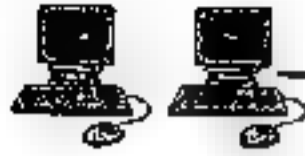
أقدم قرصنة مغاربة يلقبون بـ "قوات الردع المغربية"، على استهداف مواقع إلكترونية قطرية في أعقاب افتتاح الدورة العربية التي احتضنتها الدوحة، بسبب عرض لخريطة المملكة المغربية مستثنى منها حيزها الجغرافي الجنوبي ومن بين المواقع التي اخترقها القرصنة، منتدى سيدات الأعمال القطريات، وصفحة الفيسبوك لمونديال كرة القدم 2022 بقطر، وموقع الدورة الرياضية العربية، واعتبر القرصنة هذا الاختراق إهداء لجميع المغاربة.

كما طالبوا المسؤولين القطريين باعتذار رسمي على إظهار خريطة المغرب مبتورة خلال حفل افتتاح الألعاب العربية في قطر. وقد أثار هذا الاختراق متابعة إعلامية واسعة، انقسم بعدها الرأي العام المغربي بين مؤيد ومعارض.

تعود المغاربة ورواد الإنترنت بالخصوص على مثل هذه العمليات التي يقوم بها القرصنة المغاربة خلال السنوات الأخيرة، والتي يتابعها الإعلام بشكل متواصل. سميد بنجلي، رئيس جمعية المدونين المغاربة يعتبر أن جميع أنواع القرصنة أو الاختراق التي تهدف إلى تخريب المعطيات الرقمية أو حجب خدمات المواقع الإلكترونية، هي ممارسة جرمية حسب القانون الوطني والدولي، وقد ترتقي إلى أعمال حربية أو إرهابية إذا استهدفت أنظمة معلوماتية لها علاقة بسلامة الناس وأمنهم، ويستطرد موضحاً أنه بسبب سرعة التطور في مجال التقنيات الحديثة للإعلام والتواصل وضعف التنسيق والتعاون الدولي في الجريمة الرقمية فإن الحكومات تطبق تلك القوانين بمنطق تمييزي وانتقائي.

ويضيف بنجلي أنه من الناحية الأخلاقية فإن القرصنة يبررون أحياناً هجماتهم بكونها نضالاً من أجل الضغط على حكومات معينة أو منظمات عملاقة تجارية أو سياسية وإجبارها على تغيير موقفها من قضية معينة، وقد يكتسب فعل القرصنة مشروعيتها الأخلاقية حسب درجة أهمية القضية، لكنه يبقى فعلاً ممنوعاً قانونياً ومرتكبه يتحمل مسؤوليته الجنائية، على حد تعبير رئيس جمعية المدونين المغاربة.





أحد القرصنة المقاربة عرض للقضاء المغربي بتهمة اختراق موقع وزارة
لعدل المغربية سنة 2010 إلا أن والدافع الرئيسي وراء اختراق العديد من المواقع
المغربية مؤخراً هو "إهانة السيادة المغربية" ولكن المشكلة بالنسبة له هو الاختراق
العشوائي أي عندما يتم اختراق مواقع ليس لها صلة بالموضوع.

يروى بنجيلي أن ملونتيه تعرضتا للقرصنة من طرف جهتين متعارضتين،
الأولى تنتمي لتيار داخل حركة 20 فبراير لأنه عبر في بعض المواقف عن آراء تستند
تهاراً من الحركة، والثانية من قبل معارضي الحركة الذين اعتبروه خائن للوطن
بسبب تعبيره عن اعتراضه على سياسات الدولة.

القرصنة العراقية

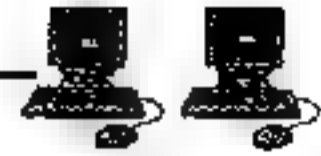
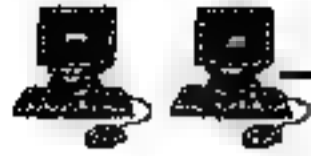
وبالرغم من عدم وجود إحصائيات دقيقة تكشف عن عدد الاختراقات
الإلكترونية في العراق إلا أن محافظة ديالى شمال شرق بغداد كشفت عن إحدى
حالات القرصنة حيث أعلنت محكمة استئناف المحافظة عن قبول دعوى قضائية
هي الأولى من نوعها في المحافظة رفعتها صحافية ضد شخص استولى على بريدها
الإلكتروني وصفحتها على موقع التواصل الاجتماعي (الفيسبوك) واستغلها
لانتحال شخصيتها.

وستعال الدعوى إلى المحاكمة وفق المادة 456 من قانون العقوبات رقم
111 لسنة 1969 التي تبلغ مدة العقوبة فيها الحبس من ثلاثة أشهر إلى خمس
سنوات كحد أقصى.

وقالت الصحافية حنين صبيحي أن مجهولاً قام بالاستيلاء على بريدها
الإلكتروني وصفحتها على فايسبوك، وطالب من خلالها ببطاقات شحن لهاتفه
النقال من لأصدقاء والمعارف مستغلاً اسمها مما جعلها في موقف "حرج".

وتنص المادة 456 من قانون العقوبات رقم 111 لسنة 1969 على أن
يعاقب بالحبس كل من توصل إلى تسلم أو نقل حيازة مال منقول مملوك للغير لنفسه
أو إلى شخص آخر وذلك بأحدى الوسائل التالية:





أ - باستعمال طرق احتيالية.

ب - باتخاذ اسم كاذب أو صفة غير صحيحة أو تقرير أمر كاذب عن واقعة معينة متى كان من شأن ذلك خدع المجنى عليه وحمله على التسليم.

وبعاقب بالعقوبة ذاتها كل من توصل باحدى الطرق السابقة الى حمل احر على تسليم او نقل حيازة سند موجد لدين او تصرف في مال او ابراء او على اي سند اخر يمكن استعماله لاثبات حقوق الملكية او اي حق عيني اخر. او توصل باحدى الطرق السابقة الى حمل اخر على توقيع مثل هذا السند او الغائه او اخلافه او تعديله.

القرصنة في الشرق الأوسط

خسائر فادحة تتكبدها منطقة الشرق الأوسط جراء عمليات الاختراق والقرصنة الإلكترونية، هذا ما أكدته المتخصصون في مجال أمن وحماية البيانات والنظم، وعبرت عنه الإحصاءات بالأرقام

حيث بلغت نحو 400 مليون دولار حتى نهاية 2009، و سجلت معدلات أكبر من مثيلاتها العالمية في زيادة عمليات الهجمات الإلكترونية، إذ زادت بنحو أربعة أضعاف مقارنة بنحو الضعفين عالمياً .

وقد ساهم الضعف في حماية المواقع الإلكترونية والبنية التحتية للمعلومات ونقص برامج التوعية والتدريب لتجنب القرصنة الإلكترونية.

وتشهد المنطقة ارتفاعاً في معدلات الاحترافات والهجمات الإلكترونية في ظل غياب قوانين فاعلة للملاحقة المتسببين في تلك الهجمات، مؤكدين أن دولاً في المنطقة مثل مصر والسعودية يتصدران قائمة ضمت دولاً عالمية حول الأكثر إصابة بفيروس «زايوس» الشهير.

وأن غياب تشريعات كافية للتصدي للجرائم الإلكترونية جعل المنطقة تحقق معدلات مرتفعة، بالإضافة إلى ارتفاع معدلات ظهور برامج وفيروسات خبيثة، إذ بلغت خلال العام الماضي نحو 1.4 مليون فيروس وبرنامج خبيث جديد مقارنة بنحو سبعة ملايين فيروس وبرنامج خبيث خلال عام 2008.





وبعد رصد هجمات فيروس «زيوس» الذي ظهر للمرة الأولى عام 2006 كانت المنطقة تتصدر قائمة الدول المتضررة عالمياً، إذ جاءت مصر في صدارة القائمة والسعودية في المركز الثالث بجانب دول خليجية أخرى. واز الإمارات لم تدخل ضمن الدول الأكثر تعرضاً لتلك الهجمات على الرغم من وجود مراكز ومؤسسات مالية عالمية عدة على أرضها، بسبب تواهر قوانين فعالة لملاحقة عصابات الجريمة الإلكترونية.

من جانبه، قال المدير الإقليمي في منطقة الشرق الأوسط لمؤسسة «كاسبرسكي لاب»، طارق كزيري، إن «حجم الخسائر المالية للهجمات الإلكترونية التي تم رصدها من قبل مؤسسات مختلفة في المنطقة خلال العام الماضي يتجاوز 400 مليون دولار»، مشيراً إلى أن «الخسائر تفوق التقديرات المعلنة، بسبب عدم إعلان شركات عن الخسائر التي تكبدتها جراء تعرضها لعمليات قرصنة إلكترونية».

مع التطور العلمي والفني والأدبي الذي أضفى سمة هذا العصر والذي هو وليد ثورات تكنولوجية واتصالية واسعة شملت مناحي الحياة برزت حاجة ملحة إلى حماية انتاجاتهم الفكرية وإبداعاتهم الذهنية وضرورة دعم قدراتهم الإبداعية الأمر الذي أسفر عن إصدار تشريع جديد يحمي تلك الانتاجات ويؤمن ضمان مصنفاتهم التي تجسدت فيها إبداعاتهم من مخاطر التقليد والمحاكاة أو القرصنة بشتى صورها . وقد أطلق على ذلك التشريع اسم (قانون حماية المؤلف) .



هوامش الفصل الخامس:

- 1 - <http://www.websy.net/learn/hackers/course49.htm>
- 2 - شبكة الاخبار التقنية بالعربي تتواصل . 2009 - 12 - 10
انظر: -
http://www.artechnews.com/index.php?page=YXJ0aWNsZQ==&op=ZGlzcGxheV9hcnRpY2xlX2RldGFpbHNfdQ==&article_id=MTI3
- 3 - صراحة صحيفة الكترونية سعودية. 11 - 07 - 2009
<http://www.sra7h.com/news-action-show-id-5157.htm>
- 4 - <http://www.alriyadh.com/2012/08/21/article761709.html>
جريدة الرياض , النسخة الالكترونية من صحيفة الرياض الصادرة عن مؤسسة اليمامة
الصحفية , الثلاثاء 3 شوال 1433 هـ اغسطس 2012 العدد 161 29
- 5 - http://www.aleqt.com/2009/08/09/article_260948.html?related
- 6 - جريدة المدى للأعلام والثقافة والفنون . الجمعة 08 - 06 - 2012 انظر: -
<http://www.almadasurements.com/news.php?action=view&id=4793>
- 7 - موقع الفيزياء التعليمي .
<http://www.hazemsakeek.net/magazine/index.php/--18426934/1203----->
- 8 - موقع امننا الاخباري . الاردن . 2012/10/8 . انظر: -
<http://amnuna.com/data.php?id=5>
- 9 - منتديات المشاغب
<http://www.absba.org/showthread.php?s=2452e1bcae147b63fd54812a9d6fa7ed&t=945238>
- 10 - روسيا اليوم . اخبار الانترنت .
http://arabic.rt.com/news_all_news/news/576567





11 رياض معروزي/الجزائر . القرصنة الالكترونية تعشش داخل الدول العربية

وخبراء ينادون . 8/4/2011 , المجلة العلمية اهرام . انظر: -

<http://ahramag.com/modules/publisher/item.php?itemid=646>

12 . جروان، فتحي . تعليم التفكير مفاهيم وتطبيقات، (ط 3)، الأردن،

عمار: دار الفكر للطباعة والنشر والتوزيع .. 7002

13 - الحارثي، ابراهيم مقبل .. الإبداع في التربية والتعليم - مرشد المعلمين

والتربويين . (مترجم)، (ط 1)، السعودية، الرياض: مكتبة الشقري للنشر

والتوزيع. 1002

14 - حوراني، مسير. تعليم مهارات التفكير. (مترجم). الإمارات، العين: دار

الكتاب الجامعي. (2002).

15 - الخطيب، جمال؛ و آخرون. مقدمة في تعليم الطلبة ذوي الحاجات الخاصة

لأردن، عمان: دار الفكر للطباعة والنشر والتوزيع.

16 - الخطيب، عامر أدوار المعلم في التربية الإبداعية بمدرسة الموهوبين. ورقة

عمل منشورة مقدمة للمؤتمر العلمي العربي الثالث لرعاية الموهوبين والمتفوقين.

الأردن، 2003.

17 - خياط، عبد اللطيف. تحسين التفكير بطريقة انقيصات الست، (ط 1،

(مترجم). الأردن، عمان: دار الأعلام.

18 - دبابسة، خلود. حاجات ومشكلات الطلبة المتميزين والموهوبين رسالة

ماجستير غير منشورة. الأردن، عمان: الجامعة الأردنية.

19 - <http://www.alnajafnews.net/najafnews/news.php?action=fullnews&.d=6851>

20 - انظر. - <http://forum.upkelk.com/t142158.html>

21 - د. توفيق السويلم . جريدة الرياض

النسخة الالكترونية من صحيفة الرياض الصادرة عن مؤسسة الإمامة الصحفية

الثلاثاء 3 شوال 1433 هـ اغسطس 2012 العدد 29 161. انظر:

<http://www.alriyadh.com/2012/08/21/article761709.html>





22 - محمد عثمان - دبي، السبت، 28 إبريل 2012 الساعة 02:53

<http://alroya.com/node/192881>

23 - عمر الحياتي، عضو الرابطة العربية للإعلاميين العلميين، اليمن - صنعاء

<http://coeia.edu.sa/index.php/ar/asuurance-awareness/articles/51-forensic-and-computer-crimes/747-war-programs.html>

24 - رابطة المرأة العراقية، القرصنة الإلكترونية في العراق: إبتزاز وتدمير مواقع

حكومية الخميس 23 - 02 - 2012 11:58 صباحا

http://iraqi womensleague.com/news_view_11088.htm

25 - هاسكرز يهتفون أكبر شركة نفط سعودية سكاي نيوز، أبو ظبي 09

سبتمبر، 2012 -

<http://www.skynewsarabia.com/web/article>

26 - <http://www.alriyadh.com/2012/10/06/article774008.html>

27 - المساء يومية اخبارية وطنية، دار الصحافة عبدالقادر سفير - لقبة

الجزائر العاصمة، 2009/12/12 انظر: -

<http://www.el-massa.com/ar/content/view/27763>

28 - <http://www.bokra.net/Articles>

29 - جريدة الشرق الاوسط، الاربعاء 01 رجب 1422 هـ 19 سبتمبر 2001

العدد 8331

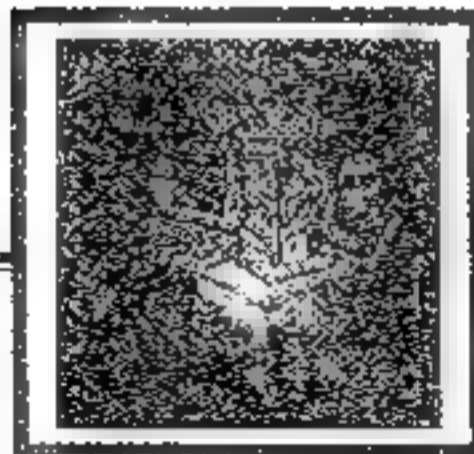
<http://www.aawsat.com/details.asp?section=6&article=57933&issueno=8331>





الفصل السادس

القرصنة الصحفية





تعرف القرصنة الصحفية: بأنها قيام بعض الصحف المحلية بسرقة مقالات وتحقيقات صحفية من صحف محلية أخرى وإعادة نشرها الأمر الذي يتقاطع مع أخلاقيات العمل الإعلامي.

وتعرف السرقة الصحفية أو ما بات يسمى "القرصنة"، بأنها قيام فيروسات السرقة بالسطو على الأعمال الصحفية المنشورة، مرتدية ثوب الذكاء أحياناً، إذ تخطف الكلمات وتدخلها لمقصلة التفسير والتحريف، وفي أحيان كثيرة تكون فيروسات غبية، تعتمد على النسخ ثم اللصق.

وتمثل الأخلاقيات والقيم المهنية للصحافة أهمية تفوق ما تمثله اللوائح والقوانين، كما تحظى في نفوس الصحفيين المهنيين بمكانة أعلى من ما تحظى به هذه اللوائح والقوانين.

فإن "الأمانة الصحفية تحتل مكانة خاصة في أخلاقيات الصحافة ومعاييرها المهنية"، فهي بمثابة حجر الزاوية في هذا المجال، وعليها يترتب مدى التزام الصحفيين بالقيم الأخرى ومراعاتهم لها من عدمه.

فمن الأمانة الصحفية يأتي الصدق في نقل الأحداث والوقائع، ومراعاة التوازن في نقل وجهات نظر أطرافها الفاعلة، ونسبة التصريحات إلى أصحابها. ومع أن هذه الظاهرة ليست جديدة في الوسط الإعلامي بعامة، إذ شهدت المؤسسات الإعلامية مثل هذه الظاهرة منذ وقت ليس بالقصير، بل قد يمتد إلى البدايات الأولى للعمل الصحفي، ولكنها بالعموم كانت من الظواهر المرفوضة والمنبوذة، وكثيراً ما دعت الجهات المتضررة منها إلى رفع الدعاوى القضائية وغيرها من الإجراءات، ما قلل من اتساعها.

وإذا كانت ظاهرة إعادة النشر اسمعت بعضاً من الكتاب في البيئات المستقرة، بوصفها تسهم في تعزيز شهرتهم وشيوع افكارهم، وإن اضرارها لن تطول سوى المؤسسات الصحفية التي تحملت التكاليف المادية للانفراد بمقالات وتحقيقات هذا الكاتب أو ذلك المحرر، إلا أن لها في البيئات غير الآمنة تبعات سلبية تطول





الكتاب والمحررين انفسهم كالاساءة الى اسمائهم، فضلا عن تعريضهم لمخاطر التصفية الجسدية وغيرها من التبعات.

وتقتصر السرقة الصحفية كذلك على المؤسسات الاعلامية الحديثة العهد بالعمل الاعلامي او قد تعجز عن تغطية احداث الساعة لافتقارها للكادر الاعلامي المتخصص او ان تتناغم وافكار احدي المؤسسات فتعمد اعادة نشرها من دون احترام حقوق الكاتب او احترام جهة النشر الاصلية.

ضحايا القرصنة الصحفية

لقد أصبح ثمة "صحفيين" يجيدون عملية النسخ واللصق أكثر من إجادتهم للعمل الصحفي.

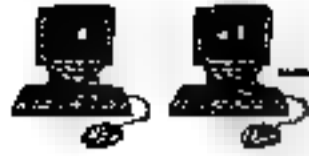
وقد انتشرت هذه الظاهرة بشكل كبير وهو ما يسيء للصحفيين، فبعض الصحفيين ممن لا يحترمون مهنة الصحافة يقوم بنقل المادة "نسخ- لصق"، وهناك كثير من الحالات هذه سواء في الصحف الورقية ام المواقع الالكترونية. والمطلوب اتخاذ اجراءات رادعة للذين يستقلون على ابواب الصحافة بجهود الآخرين.

"التصريحات الخاصة والتقارير يتم سرقتها بشكل علني ولا يتم ذكر مصدرها، ومن الطريف انه اذا وجدت أخطاء طباعية او إملائية في الموضوع يقومون بنشرها مع هذه الاخطاء.

ويشير محللون الى ان هناك صحف تحترم الحقوق الفكرية وتنسب التقارير الى مصدرها، لكن هناك صحف ومواقع إخبارية أيضا لا تحترم المهنة، وعند تواصلنا مع بعض رؤساء تحريرها يبررون سطوهم على الاخبار الى محرريهم الذين لا يملكون ناقة ولا حمل في الموضوع .

ويشير آخرون إلى ان بعض المراسلين لدى وكالات عالمية وصحف محلية وعربية وأجنبية ومواقع إخبارية يأخذون بعض المواد الصحفية التي يقوم بإعدادها محررون، حيث يقومون بنسخ المادة الصحفية ولصقها في بريده الالكتروني ومن ثم





إرسالها إلى المؤسسة الإعلامية التي يرسلها، أو يقوم بإعادة صياغتها أو تنميقها وفق الحاجة وإرسالها باسمه دون حسيب أو رقيب.

علماً أن القرصنة الصحفية بدأت تستشري بين العاملين في الصحافة وخاصة مع وجود الانترنت .

قرصنة الصور

ومع انتشار المواقع الالكترونية الإخبارية، أصبح من الصعب معرفة القرصنة الصحفية أو الصور الإخبارية.

والصحف الورقية تكون أكثر تواجداً في السوق ومن السهل معرفة الصورة المسروقة، ولكن مواقع الالكترونية صعب بعض الشيء، ويتم نشر الصور وتحت اسم صحفي آخر غير الذي التقطها فالصورة مثلها مثل الخبر، يتم القرصنة عليها.

ويتعرض عدد من مصوري المواقع الالكترونية لسطو صحفي من خلال الصور التي يتقطونها ويتم بثها عبر مراسلين لوكالات وصحف عربية وأجنبية ومحلية.

ومع ذلك "فيمكن معرفة مثل هؤلاء اللصوص بعد أن تفضحهم وسائل الإعلام المحلية التي تأخذ الصور من الوسيلة الخارجية وتنشرها في صفحاتها".

تستأثر الصورة الصحفية بأهمية خاصة في سياق التعاطي معها على صعيد السرقات الصحفية .

وذلك نظراً لأهمية الصورة والأدوار العديدة التي تؤديها سواء في المجال الصحفي، أو فيما يتعلق بالمصادقية التي تضيفها على الحدث، ومن ثم فإن الحوالب الأخلاقية والقانونية لاستخدام الصورة الصحفية تمثل جانباً مهماً في العمل الصحفي وإذا كانت التكنولوجيا قد قمت إسهامات غاية في الأهمية للصورة الصحفية، سوء فيما يتعلق بمعالجتها رقمياً، وسهولة التعامل معها إما بالحذف أو الإضافة، أو إجراء التعديلات المختلفة عليها، فضلاً عن سهولة تخزينها، وسرعة استدعائها في أي وقت، إلا أن هذه التكنولوجيا على الجانب الآخر قد سهلت أيضاً من سهولة سرقتها وتحويلها، وما يترتب عليه من إشكالية خاصة بحقوق الملكية





وتنص معظم اتفاقيات نقل الصور على ضرورة تذييل أي صورة تنشر أو ترسل أو توضع في أي مكان باسم صاحبها والمعلومات الخاصة به.

اسباب القرصنة الصحفية

أسباب السرقات الصحفية كثيرة ومتعددة أبرزها: -

- 1 - التطور التكنولوجي وسرعة انتشار الخبر.
 - 2 - وانتشار الانترنت والتقنيات الحديثة التي وفرت تربة خصبة لسوء هذه الظاهرة.
 - 3 - الانتشار الواسع للمواقع الإخبارية الإلكترونية والإعلامية.
 - 4 - الرغبة في تحقيق سبق صحفي حتى ولو كان ذلك على حساب الغير.
 - 5 - غياب الضمير لدى فئة من الصحفيين الكسالي الذين يفضلون الجلوس خلف المكاتب، أن يكافوا أنفسهم عناء النزول إلى الحياة الواقعية، وإعداد التقارير المطلوبة منهم عنها .
 - 6 - الرغبة في الحصول على رضا الرؤساء أو المؤسسة.
 - 7 - غياب القوانين والأنظمة التي تضمن حقوق الملكية وتحميها، وبخاصة بالنسبة للمواد المنشورة على شبكة الإنترنت.
- أما عواقب السرقات الصحفية فقد تكون عواقب مادية ومعنوية لمن يسرق أخبار الآخرين وهي "ملاحقتهم من قبل من تم السطو على إنتاجهم الفكري، وهذا بدوره يعرضهم لفقد الوسيلة الإعلامية التي يعملون فيها، أو يتعاملون معها".

اشكال القرصنة الصحفية

تصنف أشكال القرصنة الصحفية لعدة أصناف، منها.

- 1 - نشر أخبار ومعلومات أو تقارير صحفية دون ذكر اسم من أعدها أو نسبة الموضوع إلى شخص آخر.





2 - تجاهل الصحفي في حالة الاقتباس الصحفي وعدم الاهتمام من قبل بعض المسؤولين والإدارات الصحفية لما يخص الصحفي.

3 - سرقة الصور الصحفية والمسطو عليه من قبل مؤسسة إعلامية وتجاهل كتابة المصدر أو المصور عليها.

ويقترح خبراء الاعلام للقضاء على هذه الظاهرة "بضرورة أن يكون لدى كل صحيفة "مدونة سلوك" تنظم كل الممارسات، ويلتزم بها العاملون في الصحيفة، وإيجاد رؤية قانونية واضحة تسيير الحقوق والواجبات التي يجب مراعاتها في الأداء المهني، وأن تتصدى "نقابة الصحفيين اليمينيين" للممارسات الصحفية الخارجة على موثيق الشرف الصحفي، وأخلاقيات مهنة الصحافة وقيمها".

على الرغم من تجريم سرقة المواد الصحفية في القوانين وموئيق الشرف الصحفي في معظم التشريعات الصحفية في دول العالم إلا أن ذلك لم يحد من هذه الجرائم.

يعاني الصحفيون كثيراً من هذه الظاهرة المسببة الى المهنة والتي تعتبر الأمانة الأخلاقية من اهم شروطها.

وعلى الرغم من ان جل المواد المنشورة كانت من انتاج الصحف الكبيرة، الا ان هذه الصحف لم تحرك ساكناً في سبيل الحفاظ على حقوقها وحماية جهود محرريها وكتابها، الامر الذي قاد الى تمادي الصحف السارقة في اثمها، فيما كانت صحف اخرى تفخر بسرقة الآخرين جهودها، بوصف ذلك شهادة على جودة إنتاجها فيما تفضل بان التأثير الذي يمكن ان تحدثه تلك الرسائل قد يحسب للصحف السارقة وليس لها.

وبغية اسكات اصوات الصحفيين والكتاب المسروقة اعمالهم تقوم بعض الصحف السارقة بتثبيت اسماء اولئك الكتاب والصحفيين على مقالاتهم او تحقيقاتهم كدلالة على (الأمانة) الصحفية، لكنها في الوقت نفسه تفضل الإشارة لى جهة الشر الأولى، غير مبالية بانتهاكها لأخلاقيات العمل الإعلامي، واللامبالاة





بالأضرار التي قد تصيب الكتاب ماديا ومعنويا ، بخاصة في الاوقات التي شهدت فيها البلاد اضطرابا امتيا اخذ في جوانب منه ابعادا طائفية.

قرصنة مواقع صحفية الكترونية

المواقع الالكترونية تعرضت وتتعرض يوميا لهجمات حجب ومحو شملت مؤسسات إعلامية كبيرة وصفحات مهمة للتواصل الاجتماعي ولم تستثن المواقع والصحف العالمية فالامر ميان فاعصار القرصنة الصحفية شأنه شأن غيره من انواع القرصنة لا يعرف حدوداً ولا يقف عند حواجز طبيعية او اصطناعية . ومن هذه المواقع نذكر على سبيل المثال لا الحصر :-

قرصنة شبكة الـ "CNN" الاخبارية

كما تعرض موقع شبكة "سي إن إن" الاخبارية على الانترنت إلى عدة محاولات للاختراق تسببت بإبطاء الخدمة أو انعدامها بالنسبة لبعض المستخدمين في مناطق محدودة من آسيا

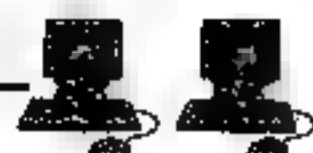
وذكرت مسئول في "سي إن إن" أن الشبكة لم تتمكن من "التعرف على المسئول عن هذا الأمر، ولا نعلم من أين أتى التشويش".

وأضاف أن المحاولة بدأت عندما أبلغت مواقع متخصصة بالكمبيوتر عن مشاكلات هاتفية من جماعات اختراق في الصين لشن هجوم بهدف وقف خدمات موقع CNN السبت، بسبب تغطية الشبكة للاشتباكات في التبت.

و اتخذت شبكة CNN إجراءات وقائية لتفالج الازدحام كرد لمحاولات تشويش وتعطيل لموقعها الإلكتروني الأمر الذي نجم عنه تأثير نسبة بسيطة من مستخدمي موقع CNN.com في آسيا.

وقال المتحدث: "بدأ يلاحظ مشاكل حوالي منتصف يوم الخميس، واتخذ إجراءات لعزل المشكلة عبر الحد من عدد المستخدمين الذين يستطيعون الدخول إليه





من مناطق جغرافية معينة ، وتابع: "أن بعض المستخدمين عانوا في هذه المناطق من صعوبات في الدخول للموقع وتصفحه".

شركة جودادى الامريكية للقرصنة

تعرضت شركة جودادى الامريكية المتخصصة في مجال بيع النطاقات الإلكترونية والاستضافة والتي تمتلك أكثر من 50 مليون نطاق إلكترونى اليوم الاثنين لعملية قرصنة ما أدى لتوقف الملايين من المواقع الإلكترونية وتمت عملية القرصنة بواسطة مجهول (AnonymousOwn3r).

وذكر عدد من المواقع التكنولوجية أن سيرفرات شركة جودادى Godaddy العالمية والكثير من المواقع التى تستضيفها قد توقفت وخاصة خدمة الـ DNS.

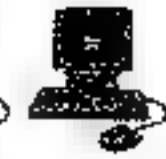
وقالت صحيفة الجارديان البريطانية إن جودادى قد تعرضت لاختراق صبح الاثنين من قبل عدد من جماعات القرصنة المجهولة دون أن يتضح عدد المواقع التى تأثرت بهذا الاختراق.

وقالت إليزابيث درسكول المتحدثة باسم الشركة فى تصريحات لموقع Cnet إن الاختراق أثر على موقع الشركة وبعض مواقع عملائها مضيفة أنه جار العمل لإعادة كل الخدمات وبدأ بعضها فى العودة فعلا.

وأكدت المتحدثة أنها لا تستطيع تحديد عدد المواقع المتأثرة بالهجوم سواء كانت آلاف أو ما إذا كانت التأثير يشمل المواقع التى تستضيفها جودادى فقط أم التى تستخدم سيرفرات DNS أيضا.

وأوضحت أن المشكلة تكمن فى عدم توافر معلومات فى الوقت الحالى. وادعى أحد القراصنة الذى أطلق على نفسه زعيم الأمن المجهول مسؤوليته بعد فترة قصيرة من الاختراق.





وقال AnonymousOwn3r كما يسمى نفسه على تويتر إنه قام باختراق جودادى لأنه يريد أن يختبر مدى الأمن الإلكتروني ولأسباب أخرى لا يستطيع أن يفصح عنها الآن.

وقال ممثلو خدمة العملاء فى جودادى على تويتر أنهم تلقوا الكثير من الشكاوى لكنهم يعملون على حل المشكلة.

وتعد شركة جودادى واحدة من أكبر مقدمى خدمات الاستضافة للمواقع على شبكة الإنترنت وتستضيف الملايين من المواقع. وتتراوح عدد النطاقات أو ال Domains التى تأثرت بهذا الاختراق ما بين مواقع صغيرة وأخرى مهمة. وتشير صحيفة الجارديان إلى أن جماعة مجهولة قامت بالاختراق هى عبارة عن مجموعة فضفاضة من المتطفلين الذين يسقون أنفسهم أون لاین ويتسللون إلى المواقع كشكل من الاحتجاج ضد حكومات أو شركات يرونها ظالمة أو فاسدة. وفى تغريدة على تويتر قال AnonymousOwn3r إنه تصرف وحده ودون تعاون مع أعضاء آخرين من تلك المجموعة. وكانت مجموعة Anonymous أو مجهول منذ إنشائها عام 2003 قد ادعت مسئوليتها عن عدد من عمليات القرصنة الكبيرة من بينها عدد من مواقع الحكومة البريطانية فى إبريل الماضى وموقع السى آى إيه فى فبراير.

المجلة المسيئة للرسول تتعرض للقرصنة الإلكترونية

مجلة شارلي ابيدو الفرنسية الساخرة التى نشرت رسوما كاريكاتورية مسيئة للنبي محمد صلى الله عليه وسلم تتعرض لعملية قرصنة منعت الدخول إليه. وقال الرسام ستيفان شاربونيه الشهير بـ«شارب» للصحفيين فى مقر الأسبوعية فى باريس «الموقع حجب لأنه تعرض لقرصنة». ويبدو أنه هجوم أوسع من ذلك الذى تعرض له عام 2011 عندما نشرت شارلي ابيدو أيضا رسوما كاريكاتورية مسيئة للنبي محمد.





وتتعرض شارلي ايبدو منذ أمس لانتقادات من ممثلي الهيئات الدينية والسياسية

ودعا شارب رئيس الوزراء الفرنسي جان مارك ايروالت إلى «دعم حرية الصحافة، والجمهورية بدلا من التأثير بعصاة من المهرجين المسخفاء الذين يتظاهرون أمام سفارة الولايات المتحدة».

وكسان شارب يشير بذلك إلى تظاهرة جرت بالقرب من مبنى السفارة الأميركية في باريس تحللتها أحداث عنف وانتهت باعتقال 150 شخصا.

وكانت المجلة الأسبوعية الساخرة نشرت في نوفمبر 2011 عددا خاصا بعنوان «شريعة ايبدو» أعلنت فيه أن النبي محمد «رئيس تحريرها»، ما أثار موجة احتجاجات وأحرقت مكاتبها وتعرض موقعها على الإنترنت إلى القرصنة. وعلى فيسبوك وتويتر، نشر المعارضون والداعمون مئات التعليقات حول الصفحة الأولى وبعضها بعبارات عنيفة جدا، وقد زار صفحة المجلة على فيسبوك إثر نشر غلاف العدد الجديد مساء الثلاثاء 1400 زائرا حتى الساعة 8.30 (6.30 نغ)

وشدد العديد من المعلقين على الظروف المتوترة جدا حاليا حيث أثار الضيلم المسيء للإسلام «براءة المسلمين» الذي أنتج في الولايات المتحدة تظاهرات مناهضة للأميركيين في العديد من دول العالم الإسلامي أسفرت عن سقوط أكثر من ثلاثين قتيلًا.

مواقع الكترونية مغربية

تعرض موقع ريف سيتي المغربية للقرصنة والسبب في ذلك راجع حسب تصريح مدير الموقع إلى عدة عمليات نجح الموقع في إفشالها في بضع دقائق لكن هذه المرة و بعد التهديدات التي تعرضت لها هيئة تحرير ريف سيتي بعد نشر خبر القنبلة التي فجرت في ضواحي العروي الذي رفض إزالته من الموقع كما رفض طلب جهات معينة في إزالة الموضوع بعدما تم نشره و ها هو الموقع يخترق لا شيء سوى لأنه حر لا يقبل المساومات





ومن جانبه أدان الصحفي عبدالجليل ادريوش المنعق العام للاتحاد العربي للصحافة الالكترونية بالمغرب هذه الجريمة التكرار، التي اعتبرها أحد وسائل كبت الحريات من خلال استخدام صلاحيات التكنولوجيا الحديثة التي تعتمد على القرصنة وسرقة المواقع الالكترونية، مؤكداً أن الاتحاد سيتخذ كافة الإجراءات الوقائية التي تحمي الحريات وتدافع عن حقوق الصحفيين العاملين بالوسائل الالكترونية. الأمر الذي يحتم ضرورة وجود قوانين رادعة لحماية الملكية الفكرية والمؤسسات الصحفية التي تعمل على الشبكة.

وطالب السيد عبدالجليل ادريوش جميع الجهات المحلية في المغرب، والمؤسسات الإقليمية والدولية بالعمل على تفعيل قوانين حماية الملكية الفكرية وحريات التعبير عن الرأي، ووضعها حيز التنفيذ لمواجهة كل أشكال القرصنة، ودعم المواقع الالكترونية الشابة التي تحترم مواثيق الشرف المهنية، وتحافظ على حقوق الملكية الفكرية.

صحيفة النهار اللبنانية

أكد وديع تويني مدير تكنولوجيا المعلومات في صحيفة النهار اللبنانية أن إسرائيل قامت بعملية قرصنة على موقعها الإلكتروني الذي ما يزال يتعرض للهجوم، حسبما نشرت وكالة الأنباء الكويتية. وأضاف تويني أن عملية القرصنة بدأت منذ أربعة أيام وتحولت إلى هجوم استهدف أحد الخوادم الرئيسية على الموقع الإلكتروني لجريدة النهار ما أدى إلى إيقافه وتعطيله، مشيراً إلى أن مصدر الهجوم والقرصنة هو إسرائيل واصفاً ما جرى بالعمل التخريبي لصحيفة تعبر عن مختلف الآراء السياسية بكل جرأة وحرية.

وتعرض الموقع الإلكتروني لصحيفة الوفد المصرية الناطقة بلسان حزب الوفد المعارض لهجوم إلكتروني من هكرز وصف نفسه بـ الهاكرز السعودي Saudi Arabia Hacker، وقام بإزالة أكثر من نصف الصفحة الرئيسية، ووضع





سلاً منها صورة لرجل ملثم يحمل مدفعاً رشاشاً مطالباً برفع شعار الصليب الموحد
أعلى الصفحة.

وقالت إدارة الموقع :إنها ظلت 3 ساعات تحاول رد اعتداء الهاكرز، ورغم
تمكنها من إعادة السيطرة على الموقع، إلا أن الهاكرز عاد وسيطر على الوضع مرة
أخري قبل أن تحل المشكلة للمرة الثانية، إلا أن صعوبة بالغة واجهت كل من حاول
الدخول إلى الموقع

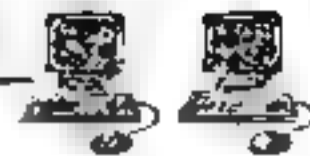
ومن المقرر أن تحرى تحقيقات داخلية في الحزب لمعرفة كيف تم الاختراق
وما هي أبعده. خاصة أن كثيرين داخل الحزب والصحيفة لم يعلموا بخبر الاختراق
الإلكتروني.

وأكد المشرف على الموقع محمد مهاود في تصريحات صحفية نقلتها
صحيفة لراية القطرية أن عملية الإصلاح والسيطرة على الموقع استمرت ساعات
عدة، قبل أن يعود إلى طبيعته، مشيراً إلى أنه فوجئ بالهاكرز يسيطر على جزء
كبير من الصفحة الرئيسية، وقد تم التعامل معه وإصلاحه

وقد مهاود :إن هناك إجراءات قانونية يتم اتخاذها بهذا الشأن من خلال
مباحث الإنترنت في وزارة الداخلية المصرية، حيث سبق لها أن تعاملت مع اختراق
مماثل تعرضت له صحيفة الأهالي الأسبوعية الناطقة بلسان حزب التجمع اليساري،
وتبين أن وراءه طالباً مازال في المرحلة الجامعية، وأنه قام بالاختراق من قبل التحربة
ليس أكثر

وأردف جوده أن "ما يلفت النظر في الاختراق المحدود الذي تم السيطرة عليه
هو الرجل الملثم الذي يحمل رشاشاً في يده والكلام المكتوب أسفل الصورة عن إزالة
الصليب من على الصفحة.





اختراق موقعي الجزيرة والعربية

وهناك العديد من الطرق المستخدمة في اختراق المواقع الالكترونية منها استغلال اخطاء في تصميم الموقع او استغلال ثغرات في السكريبتات البرمجية التي يقوم عليها الموقع و استغلال ثغرة معينة في السيرفر القائم عليه الموقع ما حديثا تستخدم فيروسات كهرومغناطيسية للهجوم على السيرفرات والمواقع

ففي عام 2003 تم اختراق موقع الجزيرة من قبل هواكر من الولايات المتحدة حيث قام المخترقون بتعديل كافة بيانات الموقع وقاموا بتحميل صورة لخريطة لولايات المتحدة الامريكية على موقع الجزيرة

صورة لموقع الجزيرة اثناء الاحراق



اختراق موقع العربية

في عام 2008 قام الجيش الالكتروني الايراني باختراق موقع العربية وحوالي 1500 موقع سعودي في نفس اليوم ردا على مجموعة من المخترقين السعوديين الذين قاموا باختراق احزاء من موقع المرجعية الدينية في إيران -
العميمتني





صورة الموقع أثناء الاختراق



اختراق موقع صحيفة، الوطن، السعودية

قام الهاكر الذي أطلق على نفسه \"Team - Dz\" باختراق الموقع، واضعاً في صدر الصفحة صورة لمضوية كبار العلماء المقال الشيخ الدكتور سعد الشثري وتحتة عدد من الأبيات مطلعها (قالوا تحفظ فإن الناس قد كثرت أقوالهم وأقوال الوري محن).

وبدت الصفحة باللون الأسود، وتم وضع عبارة \"إله إلا الله محمد رسول الله\" في رأس الصفحة، وتمت إزالتها الآن فيما يبدو أنه بداية تحرك من الجريدة لاستعادة موقعها حيث تظهر حالياً صفحة بيضاء وبها رسالة تدل على أن الصفحة تم إزالتها.

وكان مخترق الموقع قد قال أنه \"صراحة نحن لا نعرف الفرق بين الفئة الصالة من التكفيريين، وبين الطلاب الخامس أخصنة طروادة من الليبراليين فكلاهما يطمح في العلماء ويصقونهم بأقبح العبارات\". وأضاف \"أيها الشيخ الشثري إنما نحن في صفك والمخلصون كثير لكر





صوت النفاق اليوم هو الذي يدوي في صحافتنا ، فهم من القديم (إن يقولوا تسمع لقولهم) ، لكن باطلهم قصير المدى وشيك النهاية وخزائهم تنفد ، ولله حزائن السموات والأرض ولكن المتأففين لا يعلمون!.

وأكد الهاكر في أسفل الصفحة أن "الاختراق تم نصرة للشيخ المقال سعد الشثري" مع خلفية صوتية تتضمن عدد من المحاضرات الدينية. وكانت صحيفة الوطن قد نشرت حملة ضد الشيخ الشثري تضمنت عدداً من المقالات التي تستند موقفه من قضية الاختلاط في جامعة الملك عبد الله، وكان أبرزها مقال رئيس تحريرها جمال خاشقجي

من جانب ككشف رئيس التحرير جمال خاشقجي أن الاختراق الذي تعرض له موقع الصحيفة الإلكتروني قادته منظمة تعمل من الجرائر ولها فروع في مختلف أنحاء العالم وذكر منها أمريكا وإيران ودول أخرى.

وعلى صعيد متصل تعرض موقع «إرامكو السعودية»، حيث تم عزل الانظمة الإلكترونية للشركة بالكامل وإيقاف الدخول إليها من الخارج كإجراء احترازي مبكر اتخذ مع بدء العطل الطارئ الذي أصاب أمس بعض قطاعات شبكتها الإلكترونية الذي يشتبه في أنه ناشئ عن دخول فيروس إلى عدد من أجهزة الحاسب الشخصية بالشركة

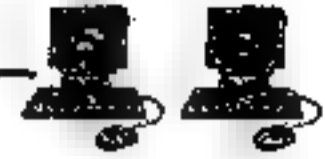
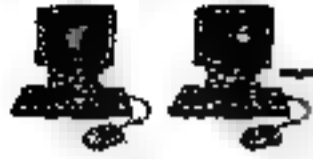
وأكدت الشركة في بيان أصدرته - سلامة الشبكة الإلكترونية المشغلة لأعمال الشركة الرئيسية للشبكة وعدم وجود أي تأثير مهما كان على أعمال الإنتاج فيها، مشيرة إلى أن وضع التشغيل الاعتيادي للشبكة. «سيعود قريباً».

وكانت وكالة «رويترز» أعلنت أن موقع التدوين الخاص بخدماتها الاخبارية تعرض لاختراق، في ما ينبئ عن عمليات قرصنة تستهدف المواقع الاخبارية

المواقع الإلكترونية الفلسطينية

المواقع الإلكترونية الفلسطينية لم تنج هي الأخرى من القرصنة فقد تعرضت وكالة الأنباء الفلسطينية الرسمية "وفا بتاريخ 31 - 1 - 2012م، منها". فضلاً عن بعض الوكالات المحلية الأخرى، حيث تم تعطيل هذه المواقع وحجبها عن الشبكة العنكبوتية.





ورغم عدم إعلان أية جهة مسؤوليتها عن هذه الهجمات، فإن خبراء ومراقبين يرجحون وقوف جهات صهيونية خلفها.

من جانبه علق وزير الاتصالات الفلسطينية، مشهور أبودقة، على عمليات القرصنة بالقول: "الموضوع ليس واضحاً بعد ويجري متابعته وما حصل هو قيام أشخاص بالدخول على مواقع فلسطينية بكثافة شديدة جداً ما تسبب في ضغط هائل على السيرفرات التي تحمل عليها هذه المواقع وبالتالي حجبتها".

وفي السياق ذاته ذكرت وكالة أنباء "عمون" الأردنية إن وكالة "معا" الإخبارية الفلسطينية تتعرض لمحاولات مكثفة لقرصنتها.

ونقلت عمون عن مصادر وصفتها بأنها "مطلعة" أن عشرات المحاولات من هـاكرز من دول مختلفة تحاول اختراق الموقع وتعطيله، وأضافت المصادر أنها لا تستبعد أن تكون محاولات قرصنة الوكالة بعد مقابلة بثتها مع رئيس الوزراء الصهيوني بنيامين نتنياهو الاثنين 30 - 1 - 2012م حيث حاول مكتب نتنياهو الضغط على العاملين فيها لسحب المقابلة.

من جانبه، قال أحد خبراء الإنترنت في تصريحات نقلها موقع "العربية نت" إن الموضوع على ما يبدو سياسياً ومبرمجاً، مرجحاً وقوف جهات صهيونية خلفه، كون أكثر من 6 موقع فلسطينية حُجبت في ذات الوقت وبنفس الطريقة، مشيراً إلى أن الأمر على ما يبدو هجوم مضاد للهجمات التي قام بها هاكرز عرب أخيراً على مواقع "إسرائيلية".

وكان فريق قرصنة فلسطيني من قطاع غزة يسمى نفسه "Gaza hacker team" قد تمكن من اختراق الموقع التابع لسلطة الإطفائية "الإسرائيلي".

ولم تقف هجمات هذا الفريق عند حد استهداف مواقع المؤسسات العامة في لـكيان الصهيوني؛ حيث اخترقوا أيضاً الموقع الرسمي لنائب وزير خارجية الكيان، داني أيلون، والذي وصف بدوره عملياته القرصنة على موقعه بأنها "فعل إرهاب" و"إعلان حرب".





وكالة انباء عراقية تفضح مؤسسات اعلامية عربية

بعد ان كانت وكالة الاخبار العراقية "واع" قد حذرت ومن خلال بيير صحفي سابق نشر على موقعها جميع المؤسسات الاعلامية التي تقوم بنقل الاخبار الخاصة بنا دون الاشارة الى مصدر الخبر، وقيام هذه المؤسسات الاعلامية بنسب هذه الاخبار لها، بما يتنافى مع اخلاقيات مهنة الصحافة .

لا ان المؤسسات المذكورة استمرت بنقل وقرصنة اخبار الوكالة ، وهو ما جعلها تقوم بفضح سياسات هذه المؤسسات الاعلامية من خلال وضع عنوان الخبر الرئيسي الذي قامت الوكالة بنشره وقائمه بأسماء المؤسسات الاعلامية التي اعتادت على قرصنة اخبارنا، وكان آخرها

خبرتم نشره عبر موقع الوكالة بتاريخ 18 أيار 2012 الموافق:

1433/6/28 هـ الساعة 8:55:08 PM

وكان تحت عنوان: نقل 20 عائلة من يهود اليمن الى اسرائيل بعد انتهاء

حكم صالح على الرابط التالي:

<http://irq4all.com/ShowNews.php?id=65215>

وتفاجأنا بأن عدد من المؤسسات الاعلامية العريقة قامت بنشر الخبر بعد ساعات من نشرنا ونصيبا عبر مواقعها الاعلامية ناسبة الخبر لها دون التتويه او الاشارة لمصدرنا في هذا الخبر ومن ضمن هذه المؤسسات الاعلامية التي سنفضح عن اسمائها ورابط نشر الخبر الذي قامت بقرصنته مع الانتباه الى تاريخ ووقت نشر هذه المؤسسات للخبر:

1- وكالة فلسطين برس

رابط نشر الخبر:

<http://www.palpress.co.uk/arabic/?action=detail&.d=48611>

2- شبكة فداء الاقصى الاعلامية رابط نشر الخبر:

<http://www.fedaagsa.com/NewsDetails.aspx?id=5261>

3- صوت فتح الاخباري رابط نشر الخبر:





<http://www.fateh-voice.ps/arabic/?action=detail&id=46301>

4- وكالة اسوار برس رابط نشر الخبر:

<http://www.aswarpress.com/ar/news.php?maa=View&id=41654>

5- شبكة العهد للاعلام رابط نشر الخبر:

<http://www.alaahd.ps/arabic/?action=detail&id=101487>

6- فلسطين بيتنا رابط نشر الخبر:

<http://www.pal-home.net/ar/categories/61483.html>

ووعدت الوكالة جميع المؤسسات الاعلامية التي تقوم بقرصنة موادها الاعلامية بملاحقتها قضائياً ان لم تلتزم بكافة معايير واخلاقيات مهنة الصحافة . ولم يقتصر الأمر على مواقع الصحف بل تعداها إلى مدونات شخصية في موقع التواصل الاجتماعي (فيس بوك) إلى الحجب.

وقال مؤسس وكالة أنباء برق ومجموعة (جكم جكم) للتواصل الاجتماعي باسم حبس أن مجهولين نجحوا في استهداف موقعيه واختراق كل إجراءات الحماية التي اتخذها للحفاظ على سرية ما فيها من معلومات.

وأكد حبس أنه الآن بصدد فتح قنوات اتصال مع جميع المواقع الالكترونية التي تعرضت لهجمات حجب لإيجاد وسيلة ناجعة في للحد منها.

اصابع الاتهام اتجهت الى القائمين في الدولة العراقية بالقيام بحجب تلك المواقع الا ان مصادر رسمية نفت ذلك مشيراً إلى أن الهجمات التي تتعرض لها المواقع العراقية إما هي من قبل مواطني دول أخرى أو عراقيون مفتربون تتنافى أفكارهم وتوجهاتهم السياسية مع أصحاب هذه المواقع، مؤكداً أن لا علاقة للدولة العراقية بهذا الأمر، لافتاً إلى ضرورة أن تتدخل الدولة العراقية والإعلان والإيضاح عن موقفها تجاه أصحاب المواقع التي تتعرض للحجب.

إلى ذلك يشير متخصصون في علوم الحاسوب والبرمجيات إلى أن المواقع الكبيرة وضعت كلمة سر تصل إلى أربعة وعشرين رقماً، ومع ذلك يتم اختراقها وحجبها، وهذا العمل لا يمكن أن يقوم به شخص حتى لو كان منمرساً في





الرمجيات، بل هو هجوم إلكتروني "كبير ومتطور" يستهدف موقع على وجه التحديد حسب أهميتها

موقع مجلة نرجس الإلكترونية العراقي تعرض لهجمة كبيرة بغية حربه، لأنه من ضمن حزمة مواقع مؤسسة المدى الإعلامية التي تعرضت لهجوم وبطريقة احترافية لا تخلو من إساءة متعمدة لشخصيات لها حضور بارز في المشهد الإعلامي.

يعمد العراق الى اتخاذ إجراءات إلكترونية لتحصين وحماية المواقع التابعة للحكومة الاتحادية من القرصنة الإلكترونية والتي تعرف بـhackers.

وزارة الاتصالات العراقية اوضحت إنها اتخذت إجراءات جديدة لصد أي محاولات اختراق إلكترونية من قراصنة مجهولين.

وقال مدير عام شركة الخدمات الدولية في وزارة الاتصالات إن شركته "اتخذت إجراءات عديدة لمنع أي اختراق للمظومة العامة للشبكة المعلومات الرسمية التي تعتمد عليها الحكومة العراقية" وكان متخصصون في مجال أمن وحماية النظم والبيانات قالوا في تقرير نشر في صيف العام الماضي إن خسائر منطقة الشرق الأوسط جرّاء عمليات الاختراق والقرصنة الإلكترونية، بلغت نحو 400 مليون دولار حتى نهاية 2009.

ويقول مبرمحو مواقع انترنت إن عمليات القرصنة تضاعفت بشكل ملفت للنظر مقارنة بالأعوام السابقة، مرجعين السبب إلى سهولة الوصول إلى البرامج المستخدمة فضلاً عن وجود مواقع ومنتديات مجانية متخصصة بتعليم الاختراق، وتسعى الحكومة العراقية إلى انجاز مشروع الحكومة الإلكترونية الذي يعتمد على الانترنت بشكل أساس في التعاملات الحكومية.

وأن "وزارة الاتصالات تعتمد على نظام البوابة الخاصة الذي يمنع أي نشاط إلكتروني غير معروف يحاول اختراق نظم المعلوماتية للحكومة العراقية"





ولم يقتصر الامر على السرقة من الصحف المحلية بل تعداه الامر الى
لصحف العربية بأخذ ملاحق كاملة واعادة نشرها دون الاشارة الى المصدر فضلا
عن اعادة نشر المواد الصحفية على اختلاف انواعها دون الاشارة الى مصدرها
وقد تأخذ السرقة الصحفية في واقع الاعلام العراقي اشكالا اخرى منها
اخذ موضوع بالكامل وإزالة اسم الكاتب ووضع اسم اخر بدلا له، وقد حصلت
حادثة ممكن انها لا تجد لها مثيلا في بقية العالم او حتى لم نسمع فيها في تاريخ
الصحافة العراقية فقد نشرت احدي الصحف العراقية مقالا افتتاحيا في الصفحة
الاولى الذي يفترض ان يكون من بنات افكار كتابها او مسؤولي النشر فادا بالمقال
الافتتاحي مسروق من موضوع سبق نشره لمسؤول القسم السياسي في صحيفة يومية
كلمة بكلمة وحرفا بحرف.

اما الانواع الاخرى للسرقات الصحفية التي بدأت تتنوع وتتطور في ظل غياب
قانون الاعلام في العراق وضعف الاجراءات الرادعة التي تتبعها نقابة الصحفيين
العراقيين، هو سرقة مقاطع من مادة صحفية وخاصة الاعمدة والمقالات او اعادة
صياغتها بتقديم وتأخير بعض الفقرات ونشرها باسماء جديدة دون رقيب او حسيب.
اما في التلفزيون فتأخذ السرقة الصحفية اشكالا اخرى منها سرقة
الافكار و الابتكارات فعلى سبيل المثال عرضت احدي الفضائيات العراقية اعلانا
تلفزيونيا تطلب فيه حاجتها الى معدي برامج وعلى المتقدمين تقديم ثلاثة افكار
لبرامج. فتقدمت فتاة بثلاثة افكار لبرامج جديدة وابدوا استحسانا لها لكنهم
اعترضوا على ميزانية البرامج التي تستوجب السفر والتنقل بين المحافظات العراقية..
وقالوا لى شكرا لك سنصل بك في وقت لاحق حال اقرار الميزانية.. وبعد بضعة
اشهر واذا بي اتفاجأ بان البرنامج عرض من على القناة دون الاشارة الى صاحب
الفكرة او معد البرنامج الحقيقي.

وهناك سرقات واضحة مثل سرقة السيوتات وبعض الابتكارات الفنية
والمقاطع التي تعتمد على القنوات الفضائية كفترات توقف في برامجها وهي كثيرة
لا مجال لذكرها هنا.





ن الوازع الذاتي بالالتزام بأخلاقيات المهنة الصحفية هو الأساس وهو الرادع لاية تجاوزات على حقوق الآخرين لكن هذا الوازع لا يكفي وحده بل من الضروري سن تشريعات وقوانين تحفظ حقوق الملكية الشخصية على مستوى النشر والاعلام او اي مجال ابداعي آخر.. ووجود مؤسسات نقابية ومهنية وحكومية يمكن اللجوء اليها لاعادة الحقوق الى اصحابها لتنظيم العمل الصحفي واعطاء صورة ايجابية ومشرقة عن مصداقية ومهنية الاعلام في العراق.

ويذكر احد الصحفيين كيف تم سرقة موضوعه واعادة نشره في احدى وكالات الانباء العراقية بالقول:

كنتُ قد أعددت تقريراً خاصاً لجريدة جدار الإلكترونيّة بعنوان "تداعيات خلية التجسس الإماراتية في سلطنة عمان" نشر بتاريخ 3- 12- 2010، حظيت صفحته بألاف القراءات وتناقلتها مواقع منسوبة لمصدرها.

وبعد ذلك بخمسة أيام نشر الموقع العراقي (شبكة نهرين الإخبارية) تقريراً بعنوان "مصادر خليجية: شبكة التجسس الإماراتية جزء من مشروع إسرائيلي لضم سلطنة عمان ما بعد مرحلة قابوس" في 8- 12- 2010، ووسمه الموقع بأنه (خاص- نهرين الإخبارية)، ودون اسم للمحرر.

إلا أن الحقيقة غير ما ادعته (الشبكة)، فالتقرير في مجمله عبارة عن نقل مباشر حريّة من مصدرين هما جريدة جدار الإلكترونيّة، وجريدة الأخبار اللبنانية (المقربة من حزب الله)، من دون مراعاة لأية قواعد في النقل والاقتباس والإشارة إلى المصادر.

وكان نصيبنا من ذلك النسخ حوالي 650 كلمة من أصل 1500 كلمة التي شكّلت حجم التقرير الخاص المزعوم. وقد أعادت نشر التقرير عشرات المواقع العربية على الإنترنت وبعض المواقع الإيرانية، وما زالت حيث قامت اليوم بإعادة نشره الزميله (وطن) الأمريكية. ولا يتحمل من أعاد نشره مسؤولية التضليل والمغالطات التي ارتكبتها (شبكة نهرين نت الإخبارية).





ويبدو أن الناسخ بعد أن تمسخ الفقرات الطوال فكر في أن يكون أميناً، وبطريقة عجن الطحين، أشار في بداية فقرة أخيرة إلى (وقال موقع عماني)؛ ليضع بهذ الأضرار الأدبية، ويؤكد على أنه ليس سيئ الخلق المهني فقط بل سيئ الإطلاع والمعرفة، وفاشل في التطبيق والسطو الأدبي إن جدار جريدة إلكترونية عربية، لا تحمل صفة قُطرية ولا تنسب نفسها إلى أي دولة. وهذا هو واقع حالها كمشروع عربي مشترك من جسيات محتملة، مفتوحة على الأفق الكوني.

لم تتوقف المفاجأة عند هذا الحد؛ فعندما أُطلعت -في حينه- إدارة التحرير على الواقعة قامت بطلب توضيح، عبر البريد الإلكتروني للموقع من المدير المسؤول: محمد جاسم خليل، عن هذا التصرف الضار والمدان الذي قام به أحد محرريه كما نفترض، إلا أنه اتضح بأن (الإيميل) المثبت في الموقع كوسيلة اتصال وحيدة لا يعمل! وقبل كتابة هذه السطور قمت بمحاولة أخرى بعد محاولة الإدارة بأسبوعين إلا أن الإيميل لا يعمل!

وهنا أول ما يتبادر إلى الذهن: كيف تعمل (شبكة إخبارية - موقع إلكتروني) على الإنترنت من دون بريد إلكتروني؟ من غير اللائق أن تتفاقم هذه الظاهرة المسيئة على الإنترنت، ومن قبل زملاء يفترض في تصديهم للعمل الإعلامي تمتعهم بدرجات أساسية من المهنية والمصداقية. فالأضرار الأدبية والمعنوية لا تلحق بنا وحدنا في جدار. بل إنها تطال آخرين يقعون تحت التضليل والخداع، وتنتج التباسات مجافية.

هذا في الوقت الذي يجابه فيه الإعلام العربي الإلكتروني تحديات عديدة على المستوى المهني والسياسي الرقابي، ويتعرض العاملون فيه إلى محاطر شتى حان وقت تخليق الإعلام العربي الإلكتروني، بما يضمن الحقوق الأدبية والفكرية والمهنية للجميع، من أجل مساهمة فعالة في دفع حركة حرية التعبير والمطالبات المدنية.





الملكية الفكرية

تعرف الملكية الفكرية بأنها حقوق امتلاك شخص ما لأعمال المكر الإبداعية أي الاختراعات والمصنفات الأدبية والفنية والرموز والأسماء والصور والنماذج والبرامج والرسوم الصناعية، التي يقوم بتأليفها أو إنتاجها.

يمكن تصنيف مكونات وحقوق الملكية الفكرية إلى مجموعتين:

1. مكونات الملكية الفكرية التقليدية: وهي المكونات والحقوق المعروفة وتتمتع بالحماية وهي: الأسرار التجارية، والبراءة، والعلاقة التجارية، وحقوق النشر.
2. المكونات والحقوق الرقمية للملكية الفكرية: ظهرت في ظل الإنترنت، ذات طبيعة رقمية وتشمل البرمجيات، قواعد البيانات، والمواقع الإلكترونية وغيرها.

الحقوق الرقمية

وتشمل:

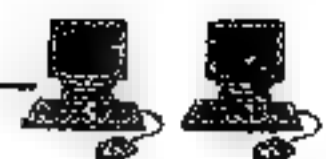
1. البرمجيات:

البرمجية (Software) خلاف الأجهزة (Hardware) فالبرمجيات هي الأساس الذي تعمل من خلاله الأجهزة لتحويلها إلى شيء مفيد يقوم بوظائف عدة مثل أنظمة التشغيل وهي من أكبر الأمثلة على البرمجيات وعلى الرغم من أن البرمجيات (بنوعها برمجيات النظام وبرمجيات التطبيق) كانت موحدة قبل الإنترنت والاستخدام التجاري الواسع لشبكات الأعمال، إلا أنها أصبحت في ظل الإنترنت تشكل القدرة العسكرية ولخبرة العظيمة التي تحرك اقتصاد المعلومات كله والمصدر الأكثر فعالية وكفاءة في صنع الثروة في الأعمال الإلكترونية. والبرمجيات هي من أكثر المنتجات الرقمية حاجة للحماية لأنها الأكثر عرضة للقرصنة.

قرصنة البرمجيات :

هي أن تقوم بنسخ البرامج واستخدامها بدون دفع ثمنها للشركة أو الشخص الذي قام بتصنيعها ؛ فالحل البديل لقرصنة البرمجيات هو استخدام البرمجيات





لحرة البرمجيات حرة المصدر هي البديل الأمثل للبرمجيات المقرصنة إن لم تود أن تدفع ثمن البرامج الأصلية . وهي برمجيات يمكن استخدامها و التعديل بها و إعادة توزيعها مجاناً بدون أي مقابل مادي بشرط عدم نسخها لأحد غير صاحبها الأصلي و يوحد برمجيات حرة المصدر ذات مستوى عالٍ من الكفاءة و يوجد أيضاً بديل حر المصدر لكل البرامج التي يقوم المستخدمون بقرصنتها فمثلاً بدل من نظام تشغيل وندوز يوجد نظام تشغيل لينكس و بدلاً من حزمة الأوفيس يوجد حزمة الأوبن أوفيس و بدل من متصفح انترنت اكسبلورر يوجد متصفح فاير فوكس و بدل من برنامج الأدوب فوتوشوب يوجد برنامج جيمب . فهذه هي فكرة البرمجيات حرة المصدر .

2- قواعد البيانات الالكترونية :

من المفترض حفظ قواعد البيانات من الاستنساخ واستغلال الآخرين فلا بد أن تكون محمية بقوانين حفظ الملكية شأنها شأن أي عمل آخر وأيضاً من الممكن حمايتها بما يسمى بحق قاعدة البيانات Database Right.

3- الموقع الالكتروني :

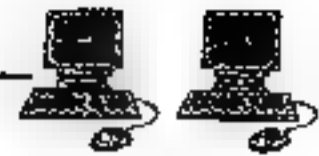
الموقع الالكتروني هو عبارة عن مجموعة من صفحات الويب ذات الصلة مع بعضها البعض، يمكن الوصول إليها عبر شبكة مثل الإنترنت أو الشبكة المحلية الخاصة.

والصفحة الواحدة تحتوي على نص أو صور أو مقاطع فيديو وغيرها وهذه الصفحة ممكن أن تشارك في الاقتناع والشراء والبيع وأغراض أخرى لا تقل أهمية عن هذه الأمور، لذا لابد أن تكون محمية بالحماية القانونية التي لا تزال غير معترف بها لمثل هذه المواقع .

ثالثاً: سرقة وقت الانترنت (internet time theft)

إن سرقة وقت الانترنت يأتي في إطار القرصنة (hacking) وهو استخدام من قبل شخص غير مصرح به لساعات للإنترنت المدفوعة من قبل شخص آخر فالقرصان يصل إلى كلمة المرور للوصول إلى الانترنت أما عن طريق القرصنة





(Internet Identity Theft) أو عن طريق وسائل غير قانونية فيحصل إلى الانترنت من دون علم أو معرفة الشخص الآخر. ونعرف -الوقت الذي تمت سرقة من قبل أي قرصان عندما ينتهي شحن الوقت ونحتاج إلى تعيئتها أو شحنها مع العلم أن الشخص لا يستخدمها بكثرة !!

إن السارق يصل إلى كلمة المرور للوصول إلى الانترنت عن طريق (Internet Identity Theft) حيث أن جهاز الكمبيوتر - مما لا نعرف عنه - أنه يقوم بجمع جميع أنواع المعلومات ويخزنها في الملفات المخفية على القرص الصلب، وهذه الملفات تقوم بتخزين المعلومات مثل تسجيل الدخول وكلمات السر، والأسماء والعناوين وحتى أرقام بطاقات الائتمان .

ويمكن الحصول على هذه المعلومات بطريقتين: إما عن طريق الاستيلاء عليها أثناء انتقالها انتقالا غير آمن بين الأجهزة عبر الشبكة أو عن طريق تثبيت برامج ضارة على جهاز الكمبيوتر الخاص بك (مثل برامج التجسس) التي من شأنها أن تجمع كل شيء تحتاج إليه تلقائيا وإعادتها إلى الجهاز مرة أخرى.

وأفضل طرق الحماية من هذا النوع :

- تأمين متصفح الويب.
- حماية المعلومات الحساسة والخاصة.
- حذف محفوظات المواقع على الإنترنت.
- حذف ذاكرة التخزين المؤقتة الخاصة بك على الجهاز.
- إفراغ سلة المحنقات.

أنواع الملكية الفكرية

يمكن تصنيف مكونات وحقوق الملكية الفكرية إلى مجموعتين:

1. مكونات الملكية الفكرية التقليدية: وهي المكونات والحقوق المعروفة وتتمتع

بالحماية وهي: الأسرار التجارية، والبراءة، والعلاقة التجارية، وحقوق النشر



2. المكونات والحقوق الرقمية للملكية الفكرية: وقد ظهرت في ظل الإنترنت، ودات طبيعة رقمية في جانبها الأهم وتشمل البرمجيات، قواعد البيانات، المواقع الإلكترونية، إلخ.

أولاً: الحقوق التقليدية للملكية الفكرية الأسرار التجارية:

إن السرية التي هي سمة الحصر في استخدام المعلومات أو تداولها تقابل مفهوم النطاق العام (Public Domain) الذي يشير إلى أن المعلومات تكون شائعة الاستخدام للجمهور.

والأسرار التجارية (Trade Secrets) هي طرق العمل وخططه وتفاعلاته، التي يتم حمايتها من خلال القانون، ومن خلال الإلزام التعاقدى المباشر. كما هو الحال في عقود استخدام العاملين التي يجب أن تتضمن تحديداً لالتزاماتهم المتعلقة بالسرية التي إن خرقوها يتعرضون للمساءلة القانونية. وهذا ما تقوم به الشركة أيضاً في اتفاقاتها مع زبائنهم في مطالبتهم بعدم كشف هذه الأسرار. وفي الوقت نفسه فإنها تعمل على حماية هذه الأسرار من التحول إلى النطاق العام.

براءة الاختراع:

إن براءة الاختراع (Patent) هي وثيقة قانونية تمنح المبتكر أو الشركة المالكة للاحتكار حقاً احتكارياً على الأفكار أو المعارف التي تتضمنها، والقابلة للتحول إلى آلة أو جهاز أو طريقة عمل أو خدمة محددة، ولا يمكن استخدامها من الآخرين إلا بإذن من المالك أو التزام تعاقدى. والبراءة هي الشكل الأكثر استخداماً والأكثر أهمية في التعبير عن الابتكارات والانجازات التكنولوجية التي كانت الأساس في التطور منذ العصر الصناعي حتى الآن.





حق النشر:

إن حق النشر أو المؤلف (Copyright) من الحقوق القديمة المحمية بالقانون. حق النشر أسهل في الحصول من براءة الاختراع، كما أن المدة الزمنية التي يغطيها هي أطول من فترة حماية البراءة وهذا ما يظهر جلياً في أن حق النشر يستمر طوال حياة المؤلف، كما أن بعض القوانين تجعل هذا الحق يستمر لمدة تمتد إلى سبعين سنة بعد موت المؤلف. ومع ذلك فإن حق النشر يتضمن كل قواعد حماية الملكية في الحق الحصري للمؤلف في عدم إعادة إنتاج العمل الخاضع لحق النشر إلا بعد أخذ الموافقة منه مع القدرة على منع الآخرين من عمل نسخ منه. وهناك شروط أساسية لا بد من توافرها في العمل الذي يحصل على حق النشر هي: التثبيت: أي أن يكون معبراً عنه بشكل مادي، والتوصل إليه أولاً كنص مكتوب كما في الجداول أو المصنفات (Compilations) كقواعد المعلومات، والوثائق، والصور، والرسوم، والأكثر حداثة يتمثل ببرامج الحاسوب.

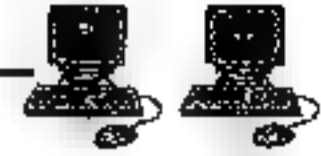
الأصالة: أن يكون العمل أصيلاً وقيمتاً أصيلة.

الحقوق المعنوية: إن العمل الإبداعي هو في جانب منه عمل مادي، يمثل المصلحة المادية للمؤلف في نشره وتقديمه وإيصاله للجمهور، وهذا ما يسمى الحق الاقتصادي الذي يحمى بالوسائل القانونية. وفي الوقت نفسه هو جزء من الملكية الفكرية للمؤلف وشخصيته الإنسانية مما يخرج عن نطاق المصلحة المادية. وكل شيء له قيمة أعلى من الملكية المادية ويوجد خارج الشخصية يمثل الحق المعنوي (Moral Right).

ولا بد من التأكيد على أن حق النشر الذي يضمن بالدرجة الأساسية الحماية القانونية للمؤلف المبدع، ترد عليه استثناءات في مقدمتها.

الاستثناء المتعلق بالاستخدام العادل (Fair Use)، كما في حالة استخدام العمل الخاضع لحق النشر لأغراض تعليمية أو نقدية أو لأغراض البحث والدراسة أو التلخيص.





إن قوانين حق النشر لا تحمي الأفكار، والمفاهيم، والمبادئ، والقوانين العلمية، والخوارزميات. والواقع أن هذا الاستثناء يقوم على عدم المبالغة في الحماية القانونية لحق النشر لأن مثل هذه المبالغة لا تحد فقط من الاستفادة من الابتكار، وإنما يمكن أن تحد من الابتكار اللاحق.

الاستثناء المتعلق بالمصلحة العامة: وهذا الاستثناء يتعلق بتجاوز حق المؤلف بعمله الإبداعي عند عزوه عن نشر هذا العمل. إذ يكون من حق السلطة العامة أن تأخذ العمل وتنشره (حتى دون رغبة المؤلف) على أن تقدم تعويضاً مناسباً لصاحبه.

الاستثناء الخاص المتعلق بالمكتبات: إن مناقشات قانون حق النشر في الألفية الرقمية (DMCA) من أجل حماية الأعمال الخاضعة لحق النشر، أكدت على التزام المكتبات بحظر استخدام التكنولوجيا الرقمية في الاستسناخ للمحافظة على الأعمال. وأقر لهذه المكتبات بعمل ثلاث نسخ فقط: نسخة الحفظ والأرشيف، والنسخة الأصلية (Master Copy)، ونسخة الاستعمال (أنظر الموقع <http://www.uspto.gov>).

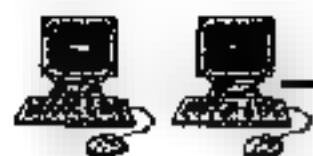
الأعمال غير المحمية: إن الأعمال الرسمية والوثائق الحكومية وأخبار اليوم والنشر في الصحف والمجلات والتقارير الإخبارية لا تتمتع بالحماية وإن كانت العادة جرت على الإشارة إليها عند عرضها أو النقل عنها.

ثانياً: الحقوق الرقمية للملكية الفكرية

إن الملكية هي الامتداد الأقوى لقدرة الفرد أو الشركة، وهذا ما يمكن أن ينطبق على حقوق الملكية الفكرية التقليدية، وعلى مكونات الملكية الفكرية لرقمية التي تسمى أيضاً الحقوق الرقمية (Digital Rights).

إن المكونات الرقمية (البرمجيات، قواعد البيانات، المواقع الإلكترونية.. إلخ) تدخل ضمن هذه الحقوق، شأنها شأن المنتجات المادية والفكرية التقليدية، إذا ما توفرت فيها شروط شمولها بالحماية القانونية. ولكن بالمقابل لا بد من مراعاة الخصائص المتميزة لهذه المكونات، وخصائص الإنترنت كشبكة عالمية سريعة الإرسال، والنسخ، والتقسيم للمعلومات وغيرها مما يؤثر على الحقوق الرقمية تأثيراً كبيراً.





هوامش الفصل السادس:

- 1 - قرصنة الانترنت يستهدفون مواقع صحفية عراقية اذاعة العراق الحر
http://www.iraqhurr.org/content/article/24628972.html 28.06.2012
- 2 - - القرصنة الصحفية .. مهنة من يدعي الصحافة 19 . الخميس، 5 مارس، 2009
انظر: * http://aseeralhazan.blogspot.com/2009/03/blog_post.html
- 3 - الكاتب العراق للجميع - 11:33:52 - 05 - 2012
http://fwww.iraq4allnews.dk/ShowNews.php?id=35445
- 4 - http://www.themenatech.com
- 5 - مفكرة الاسلام . الأحد 07 أكتوبر 2012 .
http://www.islammemo.cc/akhaber/arab/2012/10/07/156814.html
- 6 - الركن الاخضر ركن الاخبار . Friday 24-02-2012 انظر: -
http://www.grenc.com/show_news_main.cfm?id=25329
- 7 - جبار الكرعواوي السرقة الصحفية . بين التشريع وحماية السارق النجف نيوز
18/04/2012
http://www.shams-alhorreya.com/wesima_articles/index-20120418-98388.html
- 8 - نجاح العلي . جريدة الاتحاد يومية سياسية ،
http://www.alithad.com/paper.php?name=News&file=ar.ticle&sid=74450
- 9 - سمان المري - جدار الأربعاء 31 أكتوبر 2012 | 01:46 مساءً .
http://jidar.net/node/4009
- 10 - عبد الرحمن محمد الشامي . الامانة الصحفية في نقل الاخبار والمعلومات من مصادرها في ضوء حقوق الملكية الفكرية ورقة مقدمة للندوة التي ينظمها موقع التغييرات . سبتمبر . كلية الاعلام . جامعة صنعاء . 2008 .
- 11 - جابر رايد عبد الونيس بريشة . ثقافة حقوق الملكية الفكرية كلية لزراعة جامعة المنيا .
- 12 - جامعة نايف العربية للعلوم الأمنية - مركز الدراسات والبحوث . حقوق الملكية الفكرية ، الرياض 2004
- 13 - سميحة القليوبي: الملكية الصناعية ، دار النهضة العربية: القاهرة 2004





- 14 - الاتحاد العربي لحماية حقوق الملكية الفكرية - دراسة عن حقوق الملكية المكرية 2005
- 15 - الاتحاد العربي لحماية حقوق الملكية المكرية - حماية حقوق الملكية المكرية 2006
- 16 - لاتحاد العربي لحماية حقوق الملكية الفكرية الملكية المكرية في الوطن العربي 2008
- 17 - جامعة عجمان للعلوم والتكنولوجيا، الحماية القانونية لحقوق الملكية الفكرية / كتاب المؤتمر السنوي التاسع للجمعية العلمية لكليات الحقوق العربية 17 مارس 2011.
- 18 - ندوة حقوق الملكية المكرية بالأهر الشريف انظر : -
<http://mcif1.mam9.com/t221-topic>
- 19 - وحدة التخطيط الاستراتيجي وزارة التعليم العالي دليل حقوق الملكية الفكرية يناير 2007.
- 20 - تعرض موقع صحيفة النهار اللبنانية للقرصنة الاسرائيلية ، لبنان السبت 20 أكتوبر 2012 - 10:18
<http://www.ameinfo.com/ar-249348.html>
- 21 - تكنولوجيا وحاسوب ١١/٠٩/٢٠١٢ الثلاثاء ٢٥/شوال/١٤٣٣ هجري
<http://www.baghdadtimes.net/Arabic/33.php?sid=112824>
- 22 - جريدة الوطن القطرية . 2012/09/622720 الخميس
<http://www.al-watan.com/viewnews.aspx?n=C44B6C4D-FE9B-4D98-BB9E-930B42A1B28B&d=20120920>

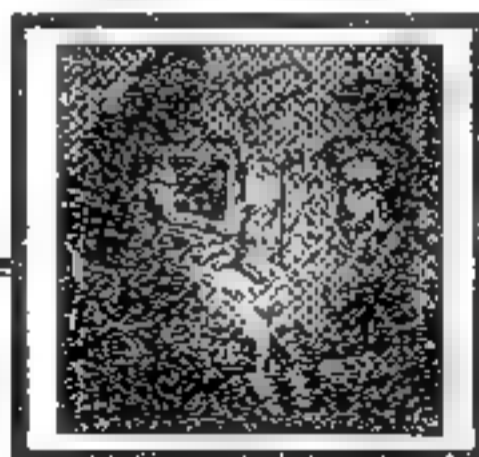




الفصل السابع

التشريعات القانونية

والقرصنة الإلكترونية





تتسارع التقنية الالكترونية بوتيرة أسرع من السوابق القانونية و يجادل بعض الخبراء بأن مطاردة المواقع الجديدة سوف تكون جهداً لا طائل تحته. ولذلك، فإن مالكي المحتوى لجأوا إلى مشغلي الموجة العريضة كأمل أخير لديهم لسيطرة على قرصنة الإنترنت. ويجادل مالكو المحتوى بأنه من خلال مراقبة زائري شبكاتهم، فإنه سوف يكون بإمكان مقدمي خدمات الإنترنت تحديد مخالفتي قوانين حقوق الطبع، وإخراج المخالفين المصريين على تكرار مخالفاتهم من إطار شبكاتهم. غير أن المفوضية الأوروبية قالت في الوقت الراهن إن منع الأفراد من الوصول إلى الإنترنت يعتبر مخالفة لحقوق الإنسان. وتبقى المنظمات الدولية والأوربية هي الأبرر في مجال إصدار تشريعات قانونية خاصة بحقوق المؤلف والحقوق المجاورة ومواكبتها للتطور التكنولوجي الحاصل في مجال المعلومات.

وهذه جولة في قوانين وتشريعات لدول العالم المتطورة و النصوص التي تعاقب جرائم القرصنة واختراق الانظمة الالكترونية، بينما لا تزال دول أخرى كثيرة تعيش في ظلام الكتروني دامس لذا لا نرى أي تشريع يخص هذا النوع من الجرائم.

السويد

تعتبر السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والانترنت، حيث صدر قانون البيانات السويدي عام (1973م) الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى شموله هضرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشروع عليها.

وتنص المادة (21) من القانون المرقم (289) والصادر في 2 نيسان 1973 الخاص بالبيانات على أن ((يعاقب كل من ولج بوسائل غير مشروعة الى سجل



مخصص لمعالجة البيانات آلياً)) من هذا يتبين أن القانون السويدي يعاقب لمجرد
الولوج غير المشروع .

أمريكا

شرعت الولايات المتحدة قانوناً خاصة بحماية أنظمة الحاسب الآلي
(1976م - 1985م)، وفي عام (1985م) حدد معهد العدالة القومي خمسة أنواع
رئيسية للجرائم المعلوماتية وهي: جرائم الحاسب الآلي الداخلية، جرائم الاستخدام
غير المشروع عن بعد، جرائم التلاعب بالحاسب الآلي، دعم التعاملات الإجرامية،
وسرقة البرامج الجاهزة والمكونات المادية للحاسب.

وفي عام (1986م) صدر قانون تشريعي يحمل الرقم (1213) عرّف فيه
جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت
المتطلبات الدستورية اللازمة لتطبيقه، وعلى أثر ذلك قامت الولايات الداخلية بإصدار
تشريعاتها الخاصة بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية تكساس
لجرائم الحاسب الآلي.

كما شرّعت قانوناً خاصاً بحماية أنظمة الحاسب الآلي وحدد معهد الدولة
القومي الأمريكي خمسة أنواع رئيسية للجرائم المعلوماتية وهي:

- جرائم الحواسيب الآلية الداخلية
- جرائم الاستخدام غير المشروع عن بعد
- جرائم التلاعب بالحاسب الآلي
- دعم التعاملات الإجرامية
- سرقة البرامج الجاهزة

وقد خولت وزارة العدل الأمريكية في عام 2000م خمس جهات حكومية
للتعامل مع جرائم الإنترنت والحاسب الآلي منها مكتب التحقيقات الفيدرالي
• FBI





بريطانيا

وتأتي بريطانيا كثال دولة تسن قوانين خاصة بجرائم الحاسب الآلي حيث أقرت قانون مكافحة التزوير والتزييف عام (1981م) الذي شمل في تعاريفه الخاصة بتعريف أداة التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى وتطبق كذلك قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والانترنت حيث عدلت في عام (1985م) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والانترنت، كما شمل القانون الجديد تحديد عقوبات المخالفات الحاسوبية، وجرائم التدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي.

في عام 1990 تم استحداث قانون يعالج فيه أساءة استخدام نظم المعلومات وقد تم بموجب هذا التشريع تجريم عملية دخول أي فرد على البيانات المخزونة في الحاسوب أو البرامج وكذلك عملية تعديلها بصورة غير مشروعة أو أي محاولة لفعل ذلك .

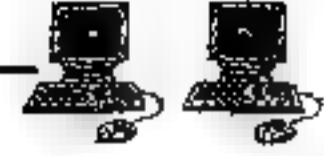
وقد نص القانون على ثلاث جرائم وهي :-

1. الدخول المتعمد غير المشروع .
2. الدخول غير المشروع والذي يتم بنية ارتكاب العديد من الجرائم .
3. القيام بأي فعل متعمد ينشأ عنه اجراء تعديل غير مشروع لمحتويات اجهزة الحاسوب .

كندا

فهي تطبق قوانين متخصصة ومفصلة للتعامل مع جرائم الانترنت، حيث عدلت في عام 1985م قانونها الجنائي؛ بحيث شمل قوانين خاصة بجرائم





الكمبيوتر والإنترنت، كما شمل القانون الجديد أيضاً تحديدًا للعقوبات المطبقة على المحالفات الإلكترونية، وأوضح القانون صلاحيات جهاز التحقيق، وحول للمأمور الضبط لقصائي حق التفتيش على أنظمة الحاسب الآلي والتعامل معها وضبطها

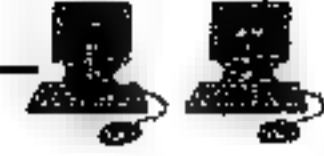
الدنمارك

طبقاً للمادة (263) من القانون الصادر في 1 حزيران 1985 - يعد من قبيل الجرائم فعل الولوج في المعلومات أو البرامج المخزونة في الحواسيب . وفي عام (1985م) سنت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلي والإنترنت والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي أو التزوير أو أي كسب غير مشروع سواء للجاني أو لطرف ثالث أو التلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها أو تغييرها أو الاستفادة منها . وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية لتتوافق مع المستجدات الإجرامية حيث أصدرت في عام (1988م) القانون رقم (19 - 88) الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها.

فرنسا

استحدث القانون الفرنسي الصادر في 5 كانون الثاني 1988 بموجب المادة (462) الفقرة الثانية من قانون العقوبات، جريمة الولوج غير المشروع في نظم المعلومات والتي تم تعديلها بموجب القانون الصادر في 29 آذار 1993 في المادة (331) الفقرة الأولى من قانون العقوبات والتي نصت ((يعاقب بالحبس لمدة سنة واحدة وبغرامة تصل إلى مائة ألف فرنك كل من تواجد أو بقي على نحو غير مشروع في نظام معالجة آلية سواء على نحو كلي أو جزئي. وتُعقد العقوبة بالحبس لمدة سنتين وبغرامة مقدارها (200.000) فرنك إذا ما ترتب على ذلك الغاء أو تعديل للبيانات التي يحتويها هذا النظام أو باختلاف وظيفة هذا النظام)).





هولندا

أما في هولندا فللقاضي التحقيق الحق بإصدار أمره بالتصنت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة.

فالنلدا

كما يجيز القانون الفنلندي لمأمور الضبط القضائي حق التصنت على المكالمات الخاصة بشبكات الحاسب الآلي، كما تعطي القوانين الألمانية الحق للقاضي بإصدار أمره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاثة أيام.

اليابان

وفي اليابان قوانين خاصة بجرائم الحاسب الآلي والانترنت ونصت تلك القوانين على أنه لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما التعاون مع جهات التحقيق أو إفشاء كلمات السر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانته.

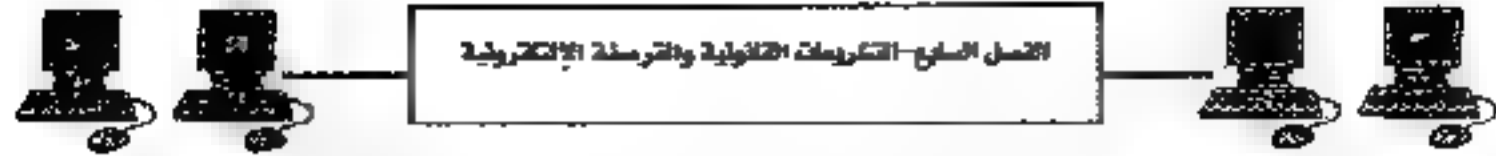
المجر وبولندا

كما يوجد في المجر وبولندا قوانين خاصة بجرائم الحاسب الآلي والانترنت توضح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها، وتعطي تلك القوانين المتهم الحق في عدم طبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الأكواد الخاصة بالبرامج.

بلجيكا

أجازت المادة 88 من القانون البلجيكي لسنة 2000 لقاضي التحقيق في حالة إمتداد البحث الإلكتروني عن أدلة الجريمة خارج نطاق بلجيكا أن يحصل





على نسخة من البيانات التي يحتاجها. وهذا معناه أن الحصول على هذه النسخة يتم دون إذن الدولة التي توجد في نطاق إقليمها البيانات المطلوبة، ويقرر الفقه البلجيكي هذا النص بالقول بأن سلطة التحقيق يمكنها الدخول إلى النظام والإطلاع على البيانات المطلوبة دون أن تترك أن هذه البيانات توجد من الناحية المادية خارج إقليم بلجيكا.

والبدل لهذا النص، هو إرسال لجنة قضائية إلى الدولة المعنية وتطلب من السلطة المختصة بها أن تحتفظ على البيانات المكونة لمحل الجريمة، وتعطيها نسخة منها، وهذا يستغرق وقتا قد يدمر خلاله المتهم هذه البيانات. ومع ذلك يعترف الفقه بأن هذا النص يمثل إعتداء على سيادة الدولة

مما تقدم يتضح لنا أن التحري والبحث والتحقيق وجميع الأدلة في مجال الجرائم الإلكترونية يكتفئ الغموض، وتحيط به العديد من الصعاب، إلا أنه لا مناص من مواصلة البحث والتحقيق وجمع الأدلة مع التطوير المستمر لوسائل البحث، ولأجهزة الشرطة وسلطات التحقيق، وتدعيم التعاون الدولي في هذا المجال.

قانون وقف القرصنة المعروف باسم (SOPA)

وهو اختصار لكلمة "Stop Online Piracy Act" قانون وقف القرصنة على الإنترنت هو قانون تم تشريعه واعتماده في الكونغرس الأمريكي وهو قانون يمنع القرصنة في الإنترنت، مما يعني وقف أي موقع على الإنترنت ينتهك مواد حقوق المصدر أو الحقوق المملوكة، أو المواد التي تساعد على عمليات القرصنة أو تقوم بعمل القرصنة، ولن يتمكن صاحب الموقع من استرجاع موقعه بل قد تصل القضية إلى محاسبته وسجنه وتغريمه، والجدير بالذكر أن هناك كوكبة من الشركات الكبيرة رفضت هذا القانون وبجسب تغييرها أنه فرض وصاية على الإنترنت وقمع الحرية.



وليس هناك من اسباب حقيقة تقف وراء سن هكذا قانون سوى رغبة امريكا في بسط نفوذها على العالم الافتراضي شركات عديدة وقفت ضد او مع هذا القانون وكل حسب مصلحته.

شركات ضخمة تقف ضد مشروع القانون الأمريكي لتحجيم الانترنت وفرض الرقابة عليه من مثل غوغل وياهو وفيس بوك وتويتر وموريل وويكيبديا وغيرها ، وتنطلق مثل هذه الشركات من أن القانون الذي يوجه لمكافحة القرصنة الالكترونية يعتمد على مبادئ مسيئة لحرية التعبير وتدفع المعلومات ولمعرفة ماهية خطورة مثل هذا القانون فعلياً في البداية قراءة ما بين سطوره.

فالقانون يمنع نشر مواد محفوظة المصدر أو مواد تساعد على القرصنة تحت طائلة إغلاق الموقع نهائياً، وحتى السجن لمدة خمس سنوات. للوهلة الأولى يبدو القانون منطقياً ولكنه لا يلحظ فترة زمنية تتيح إزالة المواد المقرصنة، بل يهدد بإغلاق الموقع بالكامل في حال وجود مواد مقرصنة عليه، الأمر الذي يسيء بشكل مباشر إلى محركات البحث ومواقع التواصل الاجتماعي بشكل رئيسي، حيث يمكن لأي مستخدم وضع مادة مقرصنة تؤدي إلى إغلاق الموقع نهائياً، وبهذا الشكل يمكن اعتبار أن موقع ويكيليكس سيفلق بحجة أنه ينشر وثائق (محفوزة المصدر) تفضح السياسة المراوغة ومواقع مثل يوتيوب إن تم نشر مقطع فيديو مخالف، والمواقع الاجتماعية إن حوت معلومات مقرصنة.

وحسب بعض المصادر فإن الرئيس الأمريكي باراك أوباما يعتبر هذا لقانون، إن تم اعتماده، قاتلاً للتطوير، في الوقت الذي رأى فيه آخرون أنه قادر على القضاء على الصحافة أيضاً، فهي تعتمد إلى نشر بعض المواد محفوظة الحقوق أو المصدر بفرض إطلاع الرأي العام عليها، وكذلك الأمر بالنسبة للمواد التي يتم نشرها في المواقع الخاصة بالمستخدمين والشركات الصغيرة، فإن تبين أن الموقع استخدم مواد تحتاج إلى تراخيص فذلك يعني إغلاق الموقع.

بعض الأصوات دعت، في حال اتخاذ مثل هذا القانون ووضعها قيد العمل، إلى الخروج من السوق الأمريكية، فيما دعا آخرون إلى مواجهة هذا القانون بموجة





احتجاجات إلكترونية بإغلاق المواقع وقد شارك في هذه الحملة مايزيد عن 7 آلاف موقع أغلقت ليوم كامل أو أقل، ومنها ما قام بنشر معلومات أو طلب بوقف بحث هذا القانون وعدم اعتماده لما يشككاه من خطورة على مستقبل العالم الرقمي. وكان قد صدر قانون الولوج المصطنع في الحاسب الآلي في تشرين الأول 1984 والذي يعاقب من ولج عمداً في حاسوب بدون إذن أو كان مسموحاً له واستغل المصلحة التي منحت له لأغراض لم يشتملها الإذن وقام عمداً بواسطة هذه الوسيلة باستعمال أو تعديل أو إتلاف أو إفشاء معلومات مخزونة في الحاسوب متى كان هذا الأخير يعمل لصالح الحكومة الأمريكية وطالما أثرت هذه الأفعال على أداء وظيفته .

تشريعات حديثة في الجرائم الإلكترونية

منذ بدء ظهور الجرائم ذات الصلة بالحاسب الآلي، تستعين الشرطة وسلطات التحقيق أو المحاكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي، وذلك بفرض كشف غموض الجريمة، أو تجميع أدلتها والتحفظ عليها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق.

وإذا كانت الاستعانة بخبير فني أمر جوازي للمحقق أو لجهة التحقيق والحكم، إلا أنه في المسائل الفنية البحتة التي لا يمكن للقاضي أن يقطع فيها برأى دون استطلاع رأي أهل الخبرة، في هذه الحالة يجب عليه أن يستعين بالخبير، فإذا تصدى للمسألة الفنية وفصل فيها دون تحقيقها بواسطة خبير كان حكمه معيباً مستوحياً نقضه، وهذا المبدأ يستقر عليه قضاء محكمة النقض المصرية.

وبناء عليه فإذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة أمر واجب على جهة التحقيق والقاضي، فهي أوجب في مجال الجرائم الإلكترونية، حيث تتعلق بمسائل فنية آية في التعقيد ومحل الجريمة فيها غير مادي، والتطور في أساليب ارتكابها سريع ومتلاحق، ولا يكشف غموضها إلا متخصص وعلى درجة





كبيرة من التميز في مجال تخصصه، فإجرام الذكاء والفن، لا يكشفه ولا يفله إلا ذكاء وفن مماثلين.

وأهمية الإستعانة بالخبير في مجال الجرائم الإلكترونية، تظهر عند غيابه، فقد تعجز الشرطة عن كشف غموض الجريمة، وقد تعجز هي أو جهة التحقق عن جميع الأدلة حول الجريمة وقد تدمر الدليل أو تمحوه بسبب الجهل أو الإهمال عند التعامل معه .

والخبير لا يشترط فيه كفاءة علمية عالية في مجال التخصص فحسب بل يجب أن يضاف إليها سنوات من أعمال الخبرة في المجال الذي تميز فيه، وعلى وجه الخصوص الجرائم ذات الصلة بالحاسب الحالي، فقد يتعلق الأمر بتزوير المستندات، أو بالتلاعب في البيانات أو الفسّاد أو نقل أو بث البيانات أو جريمة من جرائم الأموال أو الإعتداء على حرمة الحياة الخاصة، أو عرض صور أو أفلام مخلة بالآداب العامة.

ومن التشريعات الحديثة التي نظمت أعمال الخبرة في مجال الجرائم الإلكترونية، القانون البلجيكي الصادر في 23 نوفمبر سنة 2000 .

فقد نصت المادة 88 من القانون المذكور على أنه يجوز لقاضي التحقيق، وللشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفية الدخول فيه، أو الدخول للبيانات المخزنة أو المعالجة أو المنقولة بواسطته، ويعطي القانون كذلك لمسلطة للتحقيق أن تطلب من الخبير تشغيل النظام، أو البحث فيه، أو عمل نسخة من البيانات المطلوبة للتحقيق، أو سحب البيانات المخزنة أو المحولة أو المنقولة، على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق ..

ووفقا للقانون المشار إليه فإن الالتزام بتشغيل النظام واستخراج البيانات المطلوبة منه، يرجع إلى قاضي التحقيق بصفة أصلية، ويجوز ذلك للنيابة العامة على سبيل الاستثناء في حالة التلبس بالجريمة، أو عند الرضاء بعملية التفتيش هذه .





فهمة الخبير وفقاً للنص السابق تتمثل من ناحية في تشغيل النظام، ومن ناحية أخرى في تقديم البيانات المطلوبة، حسب الطريقة التي تريدها جهة التحقيق، فقد تريد البيانات مسجلة على دسك **disqu** أو على **C-DROM**، أو على الأقراص المغنطة، أو على ورق .

والتزام الخبير هو إلتزام ببذل عناية، فلا يمسأل إذا لم يصل إلى النتيجة المطلوبة نتيجة ضعف خبرته، أو بسبب العقوبات التي واجهته أثناء مباشرته لمهمته، ويمكن أن تثار مسؤوليته الجنائية إذا رفض القيام بالمهمة المكلف بها، أو ألقف عمدا البيانات المطلوب منه التعامل معها، أو حفظها .

فضلاً عن التزام الخبير بأداء مهمته التي حددتها له جهة التحقيق، يلتزم كذلك بالمحافظة على سر المهنة، وفي حالة إفشائه السر، يعاقب بالعقوبة المقررة لهذه الجريمة .

الحماية الفكرية في البلدان العربية

قد يكون لتأخر استخدام تقنيات الحاسب الآلي في الدول العربية قياساً بباقي دول العالم الأثر الكبير لتأخر إصدار تشريع يخص توفير حماية قانونية لبرامج الحاسوب من السرقة والاختراق .

الا أن أغلب الدول العربية اهتمت كثيراً بقوانين الحماية الفكرية حتى أن بعضها قد ساهم وبشكل كبير في الجهد الدولي لحماية الملكية الفكرية اعتباراً من القرن التاسع عشر .

شهدت خمسينيات القرن الماضي موجة واسعة من التشريعات التي تهتم بحماية براءات الاختراع والعلامات التجارية والتصاميم الصناعية . وكانت فترة الثمانينات قد شهدت إصدار التشريعات التي تخص حماية حق المؤلف والحقوق المجاورة أما فترة التسعينات فقد شهدت اقرار قوانين أو تعديل قوانين سابقة لتشمل برامج الحاسوب وقواعد البيانات. وفيما يلي بعض الأمثلة على هذه التشريعات



مصر

ففي مصر مثلاً لا يوجد نظام قانوني خاص بجرائم المعلومات، إلا أن القانون المصري يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعاً من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة المعلوماتية.

في القانون رقم (38) لسنة 1992 وهو تعديل للقانون المرقم (354) لسنة 1954 أصبحت فيه الحماية الفكرية تشمل مصنّفات الحاسب الآلي من برامج وقواعد بيانات وما يماثلها .

البحرين

وكذا الحال بالنسبة لمملكة البحرين فلا توجد قوانين خاصة بجرائم الإنترنت، وإن وجد نص قريب من الفعل المرتكب فإن العقوبة المنصوص عليها لا تتلاءم وحجم الأضرار المترتبة على جريمة الإنترنت.

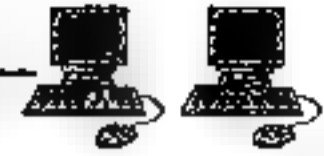
العراق

صدر امر سلطة الائتلاف رقم (83) لسنة 2004 وهو تعديل لقانون حق المؤلف رقم (3) لسنة 1971 حيث تضمنت إحدى فقراته (برامج الكمبيوتر سواء برمز المصدر أو الآلة التي يجب حمايتها كمصنّفات أدبية) .

السعودية

وفي السعودية، أعلنت السلطات المختصة أنها ستعرض عقوبات بالسجن لمدة عام واحد وغرامات لا تزيد عن 500 ألف ريال فيما يعادل 133 ألف دولار لجرائم القرصنة المرتبطة بالإنترنت وإساءة استخدام كاميرات الهواتف المحمولة مثل التقاط صور.





الإمارات

نص القانون رقم (40) لسنة 1992 المادة الثانية (يتمتع بالحماية الفكرية المقررة في هذا القانون مؤلفو المصنفات الفكرية المبتكرة في الآداب والفنون والعلوم - وشملت الفقرة (ز) من هذا القانون برامج الحاسوب) .

الأردن

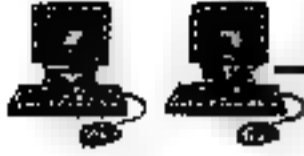
ورد في قانون حماية المؤلف رقم (22) لسنة 1992 وتعديلاته للأعوام 1998 و 1999 و 2001 الحماية القانونية للمصنفات الأدبية والفنية كما وضمت بموجبه حماية برامج الحاسوب وقواعد البيانات .

لبنان

في القانون المرقم (2385) لسنة 1924 المعدل بموجب القانون رقم (75) لسنة 1999 يحمي بموجبه جميع انتاجات العقل البشري والتي حددتها المادة لثانية ببرامج الحاسب الآلي مهما كانت لغاتها بما في ذلك الاعمال التحضيرية .

سوريا

بدأ هذا النوع من الجرائم يثير جدلا في العالم العربي وفي سورية تحديدا فمن المعروف ووفقا للقاعدة القانونية الشهيرة (لا جريمة ولا عقوبة الا بنص القانون) وباعتبار ان التشريعات العربية ومنها التشريع السوري لم يعالج هذا النوع من الجرائم الحديثة فقد بقيت هذه الافعال خارج سلطة القانون ولكن مع صدور قانون التوقيع الالكتروني وخدشات الشبكة رقم 4 تاريخ 19- 2- 2009 فقد احضرت لسلطاته بعض الجرائم الالكترونية الواقعة على الاموال (التوقيع الالكتروني) فقط دون باقي الجرائم وبالتالي ظلت الكثير من الجرائم الالكترونية خارجة عن سلطة القانون مما ينبغي التصدي لها في تشريعات خاصة



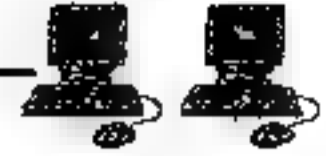
الجزائر

وتعتبر القرصنة الإلكترونية، جريمة من الجرائم المتصوص عليها في المادة 394 من قانون العقوبات الذي يعتبرها مساسا بأنظمة المعالجة الآلية للمعطيات "وكل دخول إلى نظام معلوماتي وتغيير معطياته أو سرقتها أو تخريبها"، حيث تعالج هذه الجرائم المرتبطة بالتطور التكنولوجي كبقية الجرائم على مستوى الشرطة القضائية، التي تقوم بمعاينة هذا النوع من الجرائم والبحث عن المجرمين وتقديمهم أمام العدالة، وذلك بالاعتماد على تقنيات تحقيق حديثة وتقنيين مختصين ومحققين تم تكوينهم في هذا المجال من خلال خمس دورات تكوينية تم تنظيمها منذ 2002. ولا يزال الإحجام عن تبليغ مصالح الشرطة عن الجرائم الإلكترونية المرتكبة، عائقا يحول دون التعرف على المجرمين والضحايا الذين يتعرضون للقرصنة، فضلا عما ينجر عن الحرائم الكلاسيكية المرتكبة عن طريق الوسائل التكنولوجية الحديثة للإعلام والاتصال من مشاكل كالتهريب عن طريق رسائل التهديد والرسائل المخلة بالحياة واستعمال التكنولوجيات الحديثة للترويج للإرهاب. وفي هذا الإطار أشار محافظ الشرطة عبد القادر مصطفىاوي إلى أن مصالح الشرطة القضائية تقوم بحملات تحسيس للمواطنين وتوعيتهم من أجل رفع شكاوي عند تعرضهم للقرصنة أو التهديد، وتمكين الشرطة من التحقيق في الميدان، مؤكدا على ضرورة وضع تدابير تنظيمية تخص تسيير مقاهي الانترنت وتجهيد المواقع الإباحية المفتوحة التي تستعمل في غياب الرقابة الصارمة على هذه الأخيرة.

القانون في انتظار الشكاوي والتبليغ

وحسب الأخصائيين فإن القراصنة الإلكترونيين الجرائريين قلة قليلة على عكس ما يروح عنه، فغالبية من يحترفون القرصنة هم مجموعة من المبتدئين، وعلى هذا الأساس سنت الجزائر خلال السنة الجارية، قانونا للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك في خطوة نحو ردع حرائم





المعلوماتية ، خاصة ما تعلق منها بتسخير الوسيلة التكنولوجية للترويج للإرهاب والدعاية . وبذلك تكون الحكومة قد أخذت أول خطوة نحو سد الفراغ القانوني الذي كان موجودا في مكافحة الجريمة المعلوماتية.

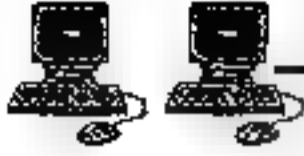
ويعد هذا القانون الذي يأتي في سياق مكافحة الإرهاب الإلكتروني بمثابة إطار قانوني مهم يحدد في بابه الأول تعريف وتحديد الجرائم المعلوماتية ثم يتقل إلى إمكانية الحد منها ومواجهتها بعد أن أصبحت تلك الجرائم من بين الجرائم التي تهدد أمن وسلامة المجتمعات، حيث جاء في 19 مادة و6 فصول تؤكد في مجملها على احترام مبدأ المحافظة على سرية الاتصالات إلا في استثناءات حددها المشروع

المغرب

وعند حديثه عن الجريمة الإلكترونية بالمغرب يؤكد المحامي المغربي إمام شقرون أن هناك قصورا في مواكبة التحولات المرتبطة بالجريمة الإلكترونية من طرف المشرع المغربي لا سيما في ظل التطور التكنولوجي الهائل، فبالرغم من تخصيصه العديد من فصول القانون الجنائي لمعاقبة بعض الجرائم الداخلة في هذا الشأن من خلال الباب العاشر المتعلق بنظم المعالجة الآلية للمعطيات سنة 2003، حيث يعاقب المشرع المغربي على دخول نظام للمعالجة الآلية للمعطيات عن طريق الاحتيال، وكذلك عرقلة سير نظام للمعالجة الآلية للمعطيات أو إحداث خلل به، و تزيف وثائق المعلومات أيا مكان شكلها إذا كان من شأن التزوير أو التزييف إلحاق ضرر بالغير.

أما بخصوص القرصنة فيفسر شقرون أن الأمر مرتبط من جهة بالنصوص المشار إليها بالقانون الجنائي المغربي ومن جهة ثانية بالقانون المتعلق بحماية الملكية بوجه عام لذي يهدف إلى وضع القواعد القانونية المقررة لحماية الإبداع الفكري، وبالتالي فإمكانية تكيف فعل القرصنة على أنه عمل إجرامي يظل مرتبطا بالأفعال المادية المرتبطة بعملية القرصنة ومخالفتها لقضايا القانون الجنائي والقوانين المتعلقة بحماية الملكية الفكرية والأدبية والصناعية والتجارية.





وهيما يتعلق بالهاكرز فيلاحظ نفس المصدر أن هناك فراغا تشريعا كبيرا في هذا الباب، فأفعال الهاكرز تقاس بمدى مخالفتها للقانون ودخولها في زمرة الأفعال المجرمة بمقتضى القانون الجنائي من جهة وتشكي أو تظلم ضحية القرصنة من جهة أخرى.

ويركز شقرون في هذا الصدد على أن المعطيات تظل قليلة جدا في هذا الصدد وتتطلب مواكبة تشريعية حقيقية خاصة وأن الجريمة الإلكترونية في وجهها المتمثل في قرصنة المواقع الإلكترونية تظل وجهها فقط من أوجه الجرائم المتعددة المتعلقة بالابتزاز مثلا.

حقوق النشر في عصر ثقافة الإنترنت

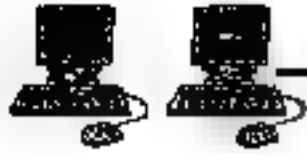
تخيل عالما يكون فيه كل كتاب، وكل أغنية، وكل برنامج، تلفزيوني وفيديو سينمائي تم إنتاجه متوافرا في الحال عبر شبكة الإنترنت بمجرد الضغط على فأرة الكمبيوتر. مثل هذا العالم يقدم وعداً ضخماً، ليس فقط للمستهلكين، لكن للفنانين والمبدعين أيضاً، الذين سيتمكنون في نهاية الأمر من الوصول إلى المشاهدين والمستمعين الذين يبعدون عنهم مسافات بعيدة، أو الذين كان الوصول إليهم مكلفاً جداً في السابق.

فقد ساعدت القرصنة على إيجاد حركة تتعلق بالتحديات القانونية والفكرية لقانون حماية حقوق الطبع.

ويقول جريجور بريور، الشريك في الإعلام الرقمي لدى شركة ريد سميث الدولية للقانون: «تحوّلت القرصنة من كونها حجة بسيطة تتعلق بالمخالفة، أو استعدام شيء ما دون إذن بذلك، إلى توجيه الأسئلة حول الأساس ذاته لحماية حقوق الطبع».

إن الرغبة في ذلك بالنسبة لمعظم جماهير الموسيقى، والأفلام، أكثر بساطة. وبامتلاك قدر قليل من المعرفة التقنية، يصبح بإمكانهم إيجاد، وتحميل، نسخ





مجاناً من أحدث الإصدارات، حيث تظهر ألبومات، وأفلام كثيرة، على الإنترنت قبل وصولها إلى المتاجر، أو إلى دور السينما.

أثبتت الإنترنت من خلال إزالتها تكاليف التوزيع، نقصها كحاضنة كاملة للقرصنة، وجعلت من الأصعب النجاح في مقاضاة أولئك المتورطين في ذلك الأمر. أشار مؤتمر الكونغرس الأمريكي لمحاربة القرصنة، هذا العام، إلى روسيا، والصين، وإسبانيا، والمكسيك، وكندا، على أن لديها أعلى معدل مخالفة قوانين حماية حقوق الطبع. ويعود ذلك بصفة رئيسية «إلى انعدام الإرادة السياسية لمواجهة المشكلة، وإن إخفاق روسيا في احترام حقوق الملكية الخاصة يهدد الآن انضمامها إلى منظمة التجارة العالمية.

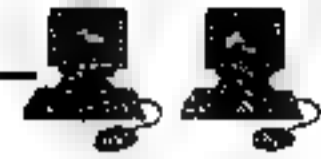
يقول جيمس بيتس، من شركة ديلويت للاستشارات: «لا يوجد في روسيا مفهوم خاص بالمادة المسجلة المحمية بحقوق النشر، حيث يمكن للروس بيعها بمجرد دفع رسوم النشر، وليس رسوم التسجيل».

إن الإحصائيات الخاصة بالمخالفات لا تبعث على الارتياح، حيث إن صناعة الموسيقى ظلت كانت مهتلة بالقرصنة على الإنترنت التي تظل الوسيلة المهمة للاستهلاك لدى الكثيرين. ومقابل كل استخدام قانوني على الإنترنت، هنالك 20 عملية تحميل غير قانونية، حسب أرقام العام الماضي، ووفقاً لما أورده جماعة الضغط الدولية للصناعة الموسيقية IFPI.

تحشى صناعة الأفلام من تكرار أخطاء صناعة الموسيقى وقد خاض تفهيدو هوليوود في هذا النقاش، بينما تضم شركات الإعلام الكبرى، مثل NBC، قواها مع نقابات العمال في الوقت الذي يعمل الارتفاع المستمر لمستويات البطالة على تركيز انتباهها على وظائف أعضائها، ودحولهم الناجمة عن مخالفات قوانين حقوق الطبع وكانت جماعة الضغط الدولية للصناعة الموسيقية تعمل مع اتحاد الصور المتحركة الأمريكي لتقاسم المعلومات حول مكافحة القرصنة وتنفيذ القوانين.

إن الإحصائيات الخاصة بذلك ليست مشجعة، حيث تم توزيع ما مجموعه 13.7 مليون فيلم عبر شبكات القرين إلى القرين في فرنسا في شهر أيار (مايو) من





عام 2008، على سبيل المثال، مقابل 12.2 مليون تذكرة سينما تم بيعها، حسب أرقام الشركتين الاستشاريتين في باريس، «إكوانسي»، و«تيرا».

غير أن صناعة الترفيه لا تقرب نفسها على الدوام من المستهلكين بأن تطرح نفسها على أساس أنها الضحية المتألمة. وقالت دراسة تمت الإشارة إلى محتوياتها على نطاق واسع في المملكة المتحدة، في هذا العام، إن التزليل يكلف الاقتصاد 120 مليار جنيه استرليني (198 مليار دولار أمريكي، أو 139 مليار يورو). وتدافعت اتحادات أخرى في هذه الصناعة لتدبب خسائرها غير أنه تبين فيما بعد أن هذا الرقم المذكور كان خاطئاً، وأن التقدير الصحيح للخسائر هو 12 مليار جنيه استرليني.

إن مثل هذه التقديرات تفترض، على وجه العموم، أن كل ألبوم يتم تحميله يعتبر صفقة بيع مفقودة، حيث تتجاهل الدراسات الأخرى التي تظهر أن معظم المخالفين الذين يمارسون التحميل، يشترون مزيداً من الموسيقى كذلك، وكان أحد قلة من الناس الذين تم توظيفهم من جانب صناعة الموسيقى، الذين قالوا إن القراصنة كانوا كذلك من أفضل زبائن مواد الموسيقى، وهو دوجلاس ميريل، قد غادر شركة EMI للموسيقى بعد أقل من عام على ذلك.

إن صناعة تقدم نفسها على أنها الضحية، بينما تقاضي الأمهات العازبات، والمستهلكين العاديين الآخرين، وتطالبهم بمبالغ كبيرة، عملت فقط على دعم قضية «بايرت بي»، وأولئك المحملين الذين يحاولون إثبات موقف فكري من خلال سرقة الموسيقى، والأفلام السينمائية. وإن أي خصم فوضوي وعدمي ينتظر أن يقدم حجة منسجمة حول كيفية الدهق مقابل إنتاج المحتوى ضمن مستقبل خال من حقوق الطبع، سوف يكون خصماً معارضاً شديداً. غير أن دوافع معظم مواقع مشاركة الملفات تحارية، وليست سياسية. وقليلون هم القراصنة الذين يريدون إنشاء شركات للتفوق على شركة يونيفرسال ميوزيك، أو شركة EMI الموسيقيتين. وهم بعملهم كمجموعة سوق تباع أقراص فيديو مدمجة، إنما يريدون فقط تحقيق بعض الأرباح من سلعة افتراضية، دون الاكتراث بالشركة التي يدمرونها من خلال ذلك، وإن ما بدأ كهواية لهووسي الكمبيوتر والمتقوهين، من أمثال شين فانتغ الذي طور «نابستار»، أصبح نشاطاً عملياً كبيراً لمالكي المواقع الإلكترونية.

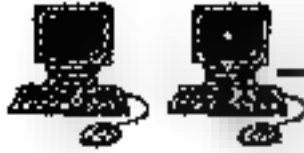




هوامش الفصل السابع:

- 1 - نوافذ . عالم الحاسوبيات . الخميس 05 رجب 1431 الموافق 17 يونيو 2010
<http://islamtoday.net/nawafeth/artshow-50-134782.htm>
- 2 عبد الله مصطفى القرصنة الإلكترونية تسبب صداما لأوروبا وتجبرها على إنشاء مركز لمواجهة في إسبانيا جريدة الشرق الأوسط . الأربعاء 13 رمضان 1433 هـ 1 أغسطس 2012 العدد 12300 .
- 3 - علا عبد الله القرصنة الإلكترونية.. جبهة جديدة للصراع في الشرق الأوسط Sat . المصري اليوم . 2012/01/28 .
<http://www.almasryalyoum.com/node/624761>
- 4 - طريق الأخبار . 200/10/10 .
<http://tags.akhbarway.com/tags.asp?q>
- 5 - البوابة . تراجع نسبة القرصنة الإلكترونية في الأردن .
<http://www.albawaba.com/ar>
- 6 - BBC Arabic . الأحد ، 22 يناير / كانون الثاني ، 2012
http://www.bbc.co.uk/arabic/middleeast/2012/01/120122_uae_hacking_thwart.shtml
- 7 - منذر سليمان . حرب وقرصنة الكترونية في الفضاء الافتراضي للشرق الأوسط وكالة أخبار الشرق الجديد . 2012 - 10 - 28
http://www.neworientnews.com/news/fullnews.php?news_id=50903
- 8 - روسيا اليوم . القرصنة الإلكترونية تهدد بنشوب حرب معلوماتية في المنطقة
http://arabic.rt.com/news_all_news/news/576561/
- 9 - عرب نت 5 .
<http://www.arabnet5.com/computer-internet-news.asp?c=2&id=161858>





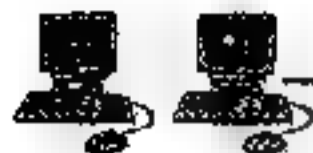
- 10 - اريبار برس . تعزيز الجهود لمحاربة القرصنة الالكترونية في الشرق الاوسط .
<http://arabic.arabianbusiness.com/business/technology/2007/sep/19/377>
- 11 - حريدة الاتحاد الحريدة المركزية للاتحاد الوطني الكردستاني العراقي
ملفات . القرصنة الالكترونية , انظر: -
<http://www.alitthad.com/paper.php?name=News&file=article&sid=99777>
- 12 - رياض معزوزي/الجزائر . القرصنة الالكترونية تعشش داخل الدول العربية
وخبراء ينادون . 8/4/2011 . المجلة العلمية اهرام . انظر: -
<http://ahramag.com/modules/publisher/item.php?itemid=646>
- 13 - الدكتور عوض محمد: المبادئ العامة في قانون الإجراءات الجنائية ، 1999
- 14 - الدكتور محمود ابو العلا عقيدة: شرح قانون الإجراءات الجنائية، ط
2001.
- 15 - الدكتور هشام رستم: قانون العقوبات ومخاطر تقنية المعلومات، 1994.
- 16 - أيوب خليل، آمنة، اتفاقية الجوانب المتصلة بالتجارة وحقوق الملكية الفردية
وأثرها على المكتبات ومراكز المعلومات في: رسالة المكتبة / جمعية المكتبات
الأردنية، مج 33 ع (حزيران 1998).
- 17 - نادي الاحياء العربي
http://alarabiclub.org/index.php?p_id=213&id=114
- 18 - احمد غنوم . دراسة حول جرائم التجارة الالكترونية من منظور قانوني
واسلامي . مؤسسة الدعوة الاسلامية الصحفية.
<http://www.aldaawah.com/?p=7056>
- 19 - <http://www.dw.de>





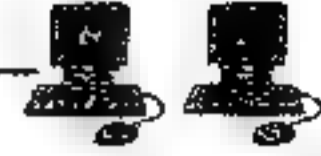
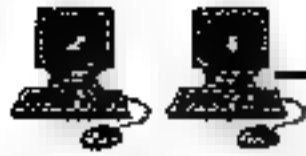
المصادر والمراجع

- 1 - محمود العريايوى . الحياة العامة و مجالات الكمبيوتر و تكنولوجيا المعلومات
هاكر ,هاكرز ,القراصنة ,اختراق ,الاختراق ,الهاكرز .انظر :
<http://kenanaonline.com/users/ELgbarbawy/posts/234859>
- 2 - ويكيبيديا الموسوعة الحرة انظر :
تم الاسترجاع من "<http://ar.wikipedia.org/w/index>."
- 3 - منتدى الحاسوب والبرامج
<http://montada.echoroukonline.com/showthread.php?t=45301>.
- 4 - منتديات صوت القرآن , 28- 08- 2006
[/http://quran.maktoob.com/vb/quran1691](http://quran.maktoob.com/vb/quran1691)
- 5 - منتديات ابن مسك .
<http://benmsik.ahlamontada.com/t118-topic>
- 6 - المصدر: شهاب النجار محاضر ومدرّب لشهادة الهاكر الاخلاقي كاتب
- 7 - المركز العربي لبحاث الفضاء الالكتروني . انظر :-
<http://www.accr.co/?p=15112>
- 8 _ عادل عبدالصديق . ملف الأهرام الإستراتيجى . ديسمبر 2007.
- 9 - المركز العربي لبحاث الفضاء الالكتروني انظر :-
<http://www.accr.co/?p=8070>
- 10 - السيد يس . جرائم الإنترنت ، دار النهضة العربية ، سنة 2000 .
- 11 - إبراهيم حامد طنطاوي . الوعي التاريخى ، الثورة الكونية ، القاهرة ، سنة 1995
- 12 - احمد حلال عز الدين . أحكام التجريم والعقاب في قانون تنظيم الاتصالات ، دار
النهضة العربية ، 2003 .
- 13 - احمد سليمان الزغاليل . اساليب التعاون العربى فى مجال التخطيط لمواجهه جرائم
الإرهاب ، الرياض ، 1414 هـ ، مشار اليه في ، المنشاوى ، دراسة جرائم الإنترنت
www.minshawwi.com ،



- 14- احمد فتحي سرور . الاتجار بالنساء والأطفال ، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها ، أكاديمية نايف العربية للعلوم الأمنية ، تونس ، 1420هـ ، مشار اليه في ، المنشاوي ، دراسة جرائم الإنترنت ، . www.minshawi.com .
- 15 - احمد حسام تمام . الوسيط في قانون الإجراءات الجنائية - دار النهضة العربية ، 1993 .
- 16- أدور غالي الذهبي . الجرائم الناشئة عن استخدام الحاسب الآلي ، القاهرة ، دار النهضة العربية ، بدون سنة نشر .
- 17- الجرائم الجنسية ، بدون ناشر ، 1997 ، الطبعة الثانية.
- 18- مجد الدين محمد بن يعقوب الفيروز ، إصدار الهيئة المصرية العامة للكتاب ، 1980 ، الجزء الرابع .
- 19- رؤوف عبيد . مبادئ الإجراءات الجنائية في القانون المصري ، القاهرة ، دار الجبل للطباعة ، الطبعة السادسة عشر ، 1985 ، ص 358.
- 20- سمير ناجي وأشرف هلال . آداب مرافعة الادعاء "أصول وممارسات" ، بدون ناشر ، 2002 ، الطبعة الأولى .
- 21- سحر الرملاوي السرقة والاحتيال وغسيل الاموال والاستغلال الجنسي والتجسس ، سبتمبر عام 2003 ، مشار اليه في ، www.alriadh.np.com
- 22- سعيد عبد اللطيف حمن . إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت ، دار النهضة العربية ، 1999 ، الطبعة الأولى.
- 23- عبد الرحمن عبد العزيز الشيفي . أمن المعلومات وجرائم الحاسب الآلي ، بدون ناشر ، 1414هـ ، الرياض الطبعة الأولى ، مشار اليه في ، المنشاوي ، دراسة جرائم الإنترنت ، www.minshawi.com
- 24- عمر الماروق الحسيني . انحراف الأحداث المشكلة والمواجهة ، بدون ناشر ، الطبعة الثانية ، 1995 .
- 25- عمر محمد يونس . الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي . بدون ناشر ، 2005 .
- 26- المجتمع المعلوماتي والحكومة الإلكترونية ، أكاكوس ، 2004





- 27 فاطمة نعناع . جريمة في فلوريدا : قضية واقعية عن استخدام شبكة الإنترنت لتدمير حياة الآخرين ، بدون ناشر ، بدون سنة نشر .
- 28 - محمود عبدالرحيم الشريفات _ " التراضي في التعاقد عبر الانترنت " _ در الثقافة للنشر والتوزيع _ سنة 2009 .
- 29 علاء السالمى " الادارة الالكترونية " _ دار وائل للنشر والتوزيع _ سنة 2008 .
- 30 بهلا المومني _ جرائم الحاسوب _ دار الثقافة للنشر والتوزيع _ سنة 2008
- 31 - رياض معزوزي/الجزائر. المجلة العلمية . اهرام . مصر
http://ahramag.com/modules/publisher/item.php?itemid=646
- 32 - http://kenanaonline.com/users/ahmedkordy/posts/320929
- 33 - جروان، فتحي الإبداع. ط1 ، الأردن، عمان :دار الفكر للطباعة والنشر والتوزيع . 2002 .
- 34 - منتديات نيابة ابن امسيك .
http://benmsik.ahlamontada.com/t118-topic
- 35 - موقع ارابيا، 10/6/2001م .
- 36 - المركز المصري لحماية الملكية الفكرية ، علي الموقع التالي:
http://www.ecipit.org.eg/Arabic/homepage_A.aspx,l/1/,2009,p.1
- 37 - http://www.alriyadh.com/2012/08/21/article761709.html . -
- 38 - جريدة الرياض . النسخة الالكترونية من صحيفة الرياض الصادرة عن مؤسسة الهمامة الصحفية . الثلاثاء 3 شوال 1433 هـ اغسطس 2012 العدد 29 161 .
- 39 - " الجرائم الإلكترونية.. الخطر الداهم على المجتمع والأسرة " على الرابط :
http://www.zoomkw.com/zoom/Article.cfm?ArticleID=76148
- أخر زيارة 13- مايو- 2010
- 40 - الحرائم الالكترونية وأنواعها والأنظمة المطبقة في السعودية " على الرابط .
http://coeia.edu.sa/index.php/ar/asuurance-awareness/articles/51-forensic-and-computer-crimes/987-types-of-electronic-crime-and-regulations-in-force-in-saudi-arabia.html , آخر زيارة 10- مايو 2010 -
- 41 - المجلة نبيل الإرهاب والانترنت " على الرابط :



www.alarabiya.net/views/2005/01/05/9306.html آخر زيارة 13 مايو 2010 -

42 Mohamed El-Guindy "East Cybercrime in the Middle East" <http://www.ask-pc.com/lessons/CYBERCRIME-MIDDLE-EAST.pdf> الرابط :

43 - الرابط :

http://fergdawg.blogspot.com/2008_03_16_archive.html آخر زيارة 13- مايو 2010.

44 - "عمليات الاحتيال المالي تكلف منطقة الخليج 380 مليون دولار". في جريدة الرياض على الرابط :

<http://www.alriyadh.com/2009/01/31/article406176.html> آخر زيارة 8- مايو - 2010

45 - "خسائرها بالمليارات .. جريمة الكترونية كل 3 دقائق على الانترنت" على الرابط :

<http://www.ensan.net/news/212/ARTICLE/3596/2008-04-22.html> آخر زيارة: 6- مايو - 2010.

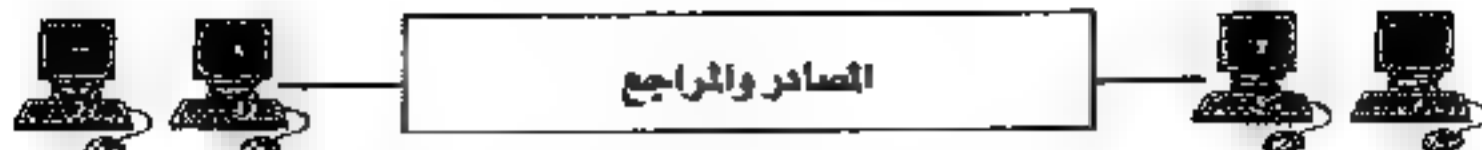
46 - العنزي، خالد. "الابتزاز" بصحيفة الإخبارية على الرابط <http://www.klb1.com/articles.php?action=show&id=229> آخر زيارة 8- مايو - 2010.

47 - الجزيرة نت، الأربعاء 1433/6/24 هـ - الموافق 2012/5/16 م انظر - : <http://www.aljazeera.net/news/pages/73658c46-12b4-4ae5-.97c4-27542cf598cf>

48 - منتديات العاصمة - 7- 10- 2009 انظر - : <http://www.3asfh.net/vb/t113052.html>

49 - جريدة الرياض ، جرائم الانترنت تعددت صورها وأشكالها فلم يعد تقتصر على اختتام الشبكات وتخريبها أو سرقة معلومات منها- تقرير: أسماء أحمد. انظر : - www.alriyadh.com



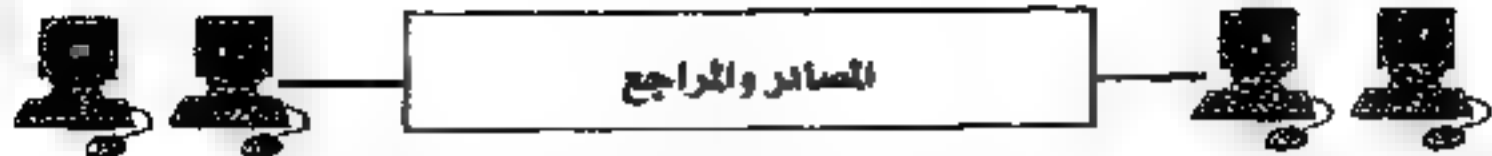


- 50 - شبكة النبا المعلوماتية - الأربعاء 17/آب/2011 - 16/رمضان/1432
- 51 - الجريمة الالكترونية للمؤلف مصطفى سمارة - مجلة المعلوماتية العدد 29 - شهر تموز 2008 .
- 52 - جمهورية العراق . السلطة القضائية . مجلس القضاء الاعلى 2012-10-15 , <http://www.iraqja.iq/view.1645>
- 53 - شاكر عبد العزيز . الحرب الالكترونية الجزء الاول الجمعية الدولية للمترجمين واللغويين العرب , 2011/01/02 انظر : <http://www.wata.cc/forums/printthread.php?s=a434fb1b04b43d2aa7686acb7b944654&ct=82289&pp=20&page=1>
- 54 - عصر الردع الالكتروني . الجزيرة نت . الجمعة 2012/10/26 م <http://www.aljazeera.net/light/6c87b8ad-70ec-47d5-b7c4-3aa56fb899e2/7bf0ab16-7011-4e73-b8ee-b756385c8a78>
- 55 - بوابة الوفد الالكتروني الوفد - المواطن الصحفي - مقال القراصنة قادمون http://www.alwafd.org/index.php?option=com_citizen&view=new&id=1831&Itemid=307
- 56 - <http://arabhardware.net/articles/software/enterprise/2458-attacks-and-hackers.html>
- 57 - صيد الفوئد , <http://www.saaaid.net/Minute/298.htm>
- 58 - <http://www.airforce-technology.com/features/feature1625>
- 59 - http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- 60 - <http://www.langner.com/en/2011/11/09/two-years-later>
- 61 - <http://www.langner.com/en/2010/10/04/stuxnet-logbook-oct-4-2010-1100-hours-mesz>
- 62 - <http://aluigi.altervista.org/adv.htm>
- 63 - http://gleg.net/agora_scada.shtml
- 64 - <http://www.itns.org.sa/Detail.asp?InSectionID=12&InNewsItemID=243>
- 65 - <http://news.ksu.edu.sa/node/35763>



- 66 <http://www.bbc.co.uk/news/technology-17623939>
- 67 - مفهوم الحرب الالكترونية . منتديات عراق السلام .
<http://www.iraqpf.com/showthread.php?t=244074>
- 68 - محمود البستاني: الاسلام وعلم الاجتماع، مجمع البحوث الاسلامية للدراسات والنشر - بيروت، الطبعة الأولى 1414هـ.
- 69 - صحيفة بوابة الشرق، عدد السبت 22 أكتوبر 2011.
- 70 - www.twitter.com
- 71 - www.adb.org/knowledgesolutions
- 73 - <http://mubde3nt.net/news-40.html>
- 74 - مشعل عبد الله القدهي: المواقع الإباحية على شبكة الانترنت وأثرها على الفرد والمجتمع، مدينة الملك عبد العزيز للعلوم والتقنية.
- 75 - عبي بن عبد الله عسيري الآثار الأمنية لاستخدام الشباب للإنترنت، ص 44.
- 76 - متفق عليه / البخاري، كتاب المناقب، باب علامات النبوة في الإسلام، حديث رقم (3411).
- 77 - مسلم، كتاب الإمارة، باب الأمر بلزوم الجماعة عند ظهور الفتن، حديث رقم (4890).
- 78 - متفق عليه / البخاري: كتاب النكاح، باب ما يتقى من شوم المرأة، حديث رقم (4808).
- 79 - مشعل عبد الله القدهي: المواقع الإباحية على شبكة الانترنت وأثرها على الفرد والمجتمع، ص 5.
- 80 - الساحة العمانية، القرصنة الإلكترونية والهاكرز وكيفية الحماية - جديد العلم والمعرفة
- 21-02-2010 <http://www.oman0.net/showthread.php/432781>
- 81 - <http://www.alriyadh.com/2011/07/20/article652259.html> 13
- 82 - هوثورن تايجل - الوجه الآخر لشبكات التواصل الاجتماعية - 20 يوليو 2011
http://coeia.edu.sa/images/stories/PDFs/Privacy_in_social_networks.pdf
- 83 - المبارك نوف - الخصوصية في الشبكات الاجتماعية - 2011/12/2
http://www.alqabas.com.kw/Temp/Pages/2011/07/20/40_page.pdf
- 84 - كبي خالد - مخاطر التواصل الاجتماعي - 20 يوليو 2011





- <http://www.tech-wd.com/wd/2010/05/24/control-your-privacy-on-facebook/>
- 85 - الضراب مازن - خصوصيتك تحت سيطرة الفيس بوك - 24 مايو 2010
- 86 - امن المعلومات انظر : - <http://security-sy.com/?p=451>
- 87 - مجران نيوز . 08 - 08 - 2011
- سعودي <http://www.sauress.com/najrannews/8632>
- خرافة شيء اسمه "امن الإنترنت"
- 88 - الجزيرة نت . الاخبار تقارير وحوارات .
- <http://www.aljazeera.net/news/pages/f2ad51ae-eb30-4af0-98c3-eb433b63fe12>
- 89 - عبد الله بن يحيى آل محيا : أثر استخدام الجيل الثاني للتعليم الالكتروني
- <http://www.facebook.com/profile.php?id=100002246432444>
- 90 - <http://www.thenewalphabet.com/radio/details3413.html>
- 91 - رؤوف اونلاين - منتديات الشروق . الفراخ التشريعي في مجال مكافحة الجرائم الالكترونية . 05 - 07 - 2007 . انظر : -
- <http://montada.echoroukonline.com/showthread.php?s=ce1d1dec60d010e871230ecdce6e4360&t=7916>
- 92 - لخطار الامنية للانترنت . منتديات الشروق . 09 - 11 - 2008
- <http://montada.echoroukonline.com/showthread.php?s=ce1d1dec60d010e871230ecdce6e4360&t=45297>
- 93 - موقع هيئة تقنية المعلومات . سلطنة عمان . October 08, 2012 . انظر :
- http://www.ita.gov.om/ITAPortal_AR/Pages/Page.aspx?NID=1&PID=8&LID=4
- 94 - الامارات اليوم - التكنولوجيا الرقمية تواكب لتطور 2012 / 9 / 4
- <http://www.emaratalyoun.com/local-section/2008-05-31-1.199487>
- 95 - <http://www.websy.net/learn/hackers/course49.htm>
- 96 - شبكة الاخبار التقنية بالعربي نتواصل . 10-12-2009 انظر : -
- http://www.artechnews.com/index.php?page=YXJ0aWNsZQ==&op=ZGlzcGxheV9hcnRpY2xlX2RldGFpbHNfdQ==&article_id=MTI3
- 97 - صراحة صحيفة الكترونية سعودية . 11 - 07 - 2009

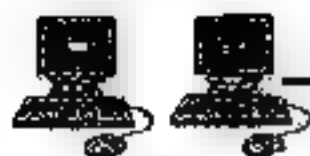


- <http://www.sra7h.com/news-action-show-id-5157.htm>
<http://www.alriyadh.com/2012/08/21/article761709.html> 98
 جريدة الرياض - النسخة الالكترونية من صحيفة الرياض الصادرة عن مؤسسة البصمة
 الصحفية الثلاثاء 3 شوال 1433 هـ - أغسطس 2012 العدد 161 29
http://www.alcqt.com/2009/08/09/article_260948.html?related - 99
 100 - جريدة المدى للأعلام والثقافة والفنون . الجمعة 08 - 06 2012 ، انظر
<http://www.almadasupplements.com/news.php?action=view&id=47>
 . 93
 101 - موقع الفيزياء التعليمي .
<http://www.hazemsakeek.net/magazine/index.php/-->
 - - - - - 18426934/1203
 102 - موقع امننا الاخباري . الاردن . 2012/10/8 ، انظر . -
<http://amnuna.com/data.php?id=5>
 103 - منتديات المشاغب
<http://www.absba.org/showthread.php?s=2452e1bcae147b63fd54812a9d6fa7ed&t=945238>
 104 - روسيا اليوم . اخبار الانترنت .
http://arabic.rt.com/news_all_news/news/576567
 105 - رياض معزوزي/الجزائر . القرصنة الالكترونية تفسح داخل الدول العربية
 وخبراء ينادون 8/4/2011 . المجلة العلمية اهرام . انظر : -
<http://ahramag.com/modules/publisher/item.php?itemid=646>
 106 - جروان ، فتحي . تعليم التفكير مفاهيم وتطبيقات ، (ط 3) ، الأردن ،
 عمان : دار الفكر للطباعة والنشر والتوزيع .
 7002
 107 - الحارثي ، ابراهيم مقبل . الإبداع في التربية والتعليم - مرشد المعلمين
 والتربويين (. مترجم) ، (ط 1) ، السعودية ، الرياض : مكتبة الشقري للنشر والتوزيع .
 1002
 108 - حوراني ، منير . تعليم مهارات التفكير (. مترجم) . الإمارات ، العين : دار
 الكتاب الحامدي . (2002) .
 109 - الخطيب ، جمال ؛ و آخرون . مقدمة في تعليم الطلبة ذوي الحاجات الخاصة .
 الأردن ، عمان : دار الفكر للطباعة والنشر والتوزيع .





- 110 الخطيب، عامر. أدوار المعلم في التربية الإبداعية بمرحلة الموهوبين ورقة عمل منشورة مقدمة للمؤتمر العلمي العربي الثالث لرعاية الموهوبين والمتفوقين . الأردن، 2003.
- 111 خياط، عبد اللطيف. تحسين التفكير بطريقة القبعات الست، (ط1) ، (مترجم)، الأردن، عمان: دار الأعلام.
- 112 دبابية، خلود. حاجات ومشكلات الطلبة المتميزين والموهوبين. رسالة ماجستير غير منشورة، الأردن، عمان: الجامعة الأردنية.
- 113 - <http://www.alnajafnews.net/najafnews/news.php?action=fullnews&id=6851>
- 114 - <http://forum.upkelk.com/t142158.html> انظر؛
- 115 - د. توفيق السويلم، جريدة الرياض النسخة الالكترونية من صحيفة الرياض الصادرة عن مؤسسة اليمامة الصحفية الثلاثاء 3 شوال 1433 هـ أغسطس 2012 العدد 16129. انظر : - <http://www.alnyadh.com/2012/08/21/article761709.html>
- 116 - قرصنة الانترنت يستهدفون مواقع صحفية عراقية اذاعة العراق الحر 28.06.2012 <http://www.iraqhurr.org/content/article/24628972.html>
- 117 - القرصنة الصحفية .. مهنة من يدعي الصحافة 14، الخميس، 5 مارس، 2009 انظر : - <http://aseeralhzan.blogspot.com/2009/03/blog-post.html>
- 118 - الكاتب : العراق للجميع - 11:33:52 2012 - 05 - 19 <http://fwww.iraq4allnews.dk/ShowNews.php?id=35445>
- 119 - <http://www.themenatech.com/>
- 120 - مفكرة الاسلام، الأحد 07 أكتوبر 2012، <http://www.islammemo.cc/akhbar/arab/2012/10/07/156814.html>
- 121 - الركن الاخضر، ركن الاخبار، Friday 24-02-2012 انظر : - http://www.grenc.com/show_news_main.cfm?id=25329



- 122 - جبار الكرعاني . العرقلة الصحفية ..بين التشريع وحماية السارق . النجف نيوز 18/04/2012
http://www.shams-alhorreya.com/wesima_articles/index_20120418-98388.html
- 123 - نجاح العلي . جريدة الاتحاد يومية سياسية .
<http://www.alitthad.com/paper.php?name=News&file=article&sid=74450>
- 124 - سلمان المري - جدار . الأربعاء 31 أكتوبر 2012 | 01:46 مساءً
<http://jidar.net/node/4009>
- 125 - عبد الرحمن محمد الشامي الامانة الصحفية في نقل الاخبار والمعلومات من مصادرها في ضوء حقوق الملكية الفكرية ورقة مقدمة للندوة التي ينظمها موقع التغيرنت سبتمبر . كلية الاعلام . جامعة صنعاء . 2008 .
- 126 - جابر زايد عبد الوهيس بريشة . ثقافة حقوق الملكية الفكرية . كلية الزراعة جامعة المنيا .
- 127 - جامعة نايف العربية للعلوم الأمنية - مركز الدراسات والبحوث: حقوق الملكية الفكرية ، الرياض 2004
- 128 - سميرة القليوبي: الملكية الصناعية ، دار النهضة العربية: القاهرة 2004
- 129 - الاتحاد العربي لحماية حقوق الملكية الفكرية - دراسة عن حقوق الملكية الفكرية 2005
- 130 - الاتحاد العربي لحماية حقوق الملكية الفكرية - حماية حقوق الملكية الفكرية . 2006 .
- 131 - الاتحاد العربي لحماية حقوق الملكية الفكرية - الملكية الفكرية في الوطن العربي 2008
- 132 - جامعة عجمان للعلوم والتكنولوجيا ، الحماية القانونية لحقوق الملكية الفكرية / كتاب المؤتمر السنوي التاسع للجمعية العلمية لكليات الحقوق العربية 17 مارس 2011 .
- 133 - ندوة حقوق الملكية الفكرية بالأزهر الشريف انظر : -
<http://mcif1.mam9.com/t221-topic>
- 134 - وحدة التخطيط الاستراتيجي . وزارة التعليم العالي . دليل حقوق الملكية الفكرية . يناير 2007 .





- 135 - تعرض موقع صحيفة النهار اللبنانية للقرصنة الإسرائيلية . لبنان السبت 20 أكتوبر 2012 - 10:18
<http://www.ameinfo.com/ar-249348.html>
- 136 - تكنولوجيا وحاسوب ١١/٠٩/٢٠١٢ الثلاثاء ٢٥/شوال/١٤٣٣ هجري
<http://www.baghdadtimes.net/Arabic/33.php?sid=112824>
- 137 - جريدة الوطن القطرية 6227 2012/09/20 الخميس
<http://www.al-watan.com/viewnews.aspx?n=C44B6C4D-FE9B-4D98-BB9E-930B42A1B28B&d=20120920>
- 138 - نوافذ عالم الحاسوبيات الخميس 05 رجب 1431 الموافق 17 يونيو 2010
<http://islamtoday.net/nawafeth/artshow-50-134782.htm>
- 139 - عبد الله مصطفى . القرصنة الإلكترونية تسبب صداما لأوروبا وتجبرها على إنشاء مركز لمواجهة في إسبانيا . جريدة الشرق الأوسط الأربعاء 13 رمضان 1433 هـ 1 أغسطس 2012 العدد 12300 .
- 140 - علا عبد الله القرصنة الإلكترونية، جبهة جديدة للصراع في الشرق الأوسط . Sat، المصري اليوم . 2012/01/28
<http://www.almasryalyoum.com/node/624761>
- 141 - طريق، لاخبار، 200/10/10 . <http://tags.akhbarway.com/tags.asp?q> .
- 142 - البوابة، تراجع نسبة القرصنة الإلكترونية في الأردن .
<http://www.albawaba.com/ar>
- 143 - BBC Arabic، لأحد، 22 يناير/ كانون الثاني، 2012
http://www.bbc.co.uk/arabic/middleeast/2012/01/120122_uae_hackin_g_thwart.shtml
- 144 - منذر سليمان، حرب وقرصنة إلكترونية في الفضاء الافتراضي للشرق الأوسط
وكالة أخبار الشرق الجديد، 2012 - 10 - 28
http://www.neworientnews.com/news/fullnews.php?news_id=50903



- 145 - روسيا اليوم القرصنة الالكترونية تهدد بنشوب حرب معلوماتية في المنطقة
http://arabic.rt.com/news_all_news/news/576561/ .
- 146 - عرب نت 5 . [http://www.arabnet5.com/computer-internet-](http://www.arabnet5.com/computer-internet-news.asp?c=2&id=161858)
[news.asp?c=2&id=161858](http://www.arabnet5.com/computer-internet-news.asp?c=2&id=161858) .
- 147 - ارييان برس ، تعزيز الجهود لمحاربة القرصنة الالكترونية في الشرق الاوسط
[http://arabic.arabianbusiness.com/business/technology/2007/sep/](http://arabic.arabianbusiness.com/business/technology/2007/sep/19/377)
[19/377](http://arabic.arabianbusiness.com/business/technology/2007/sep/19/377) .
- 148 - جريدة الاتحاد الجريدة المركزية للاتحاد الوطني الكردستاني العراقي ، ملومات
 القرصنة الالكترونية ، انظر : -
<http://www.alitthad.com/paper.php?name=News&file=article&si>
[d=99777](http://www.alitthad.com/paper.php?name=News&file=article&si) .
- 149 - رياض معزوزي/الجرائر ، القرصنة الالكترونية تعشش داخل الدول العربية
 وخبراء ينادون ، 8/4/2011 ، المجلة العلمية اهرام ، انظر : -
<http://ahramag.com/modules/publisher/item.php?itemid=646>
- 23 - الدكتور عوض محمد : المبادئ العامة في قانون الإجراءات الجنائية ، 1999 .
- 150 - الدكتور محمود ابو العلا عقيدة : شرح قانون الإجراءات الجنائية ، ط
 2001 .
- 151 - الدكتور هشام رستم : قانون العقوبات ومحاطر تقنية المعلومات ، 1994
- 152 - ايوب خليل ، آمنة ، اتفاقية الجوانب المتصلة بالتجارة وحقوق الملكية الفردية
 وأثرها على المكتبات ومراكز المعلومات في: رسالة المكتبة / جمعية المكتبات
 الأردنية ، مج 33 ع (حزيران 1998) .
- 153 - نادي الاحياء العربي
http://alarabiclub.org/index.php?p_id=213&id=114
- 154 - احمد غيوم . دراسة حول جرائم التجارة الالكترونية من منظور قانوني وسلامي
 مؤسسة الدعوة الاسلامية الصحفية .
<http://www.aldaawah.com/?p=7056>
- 155 - جمال غيطاس ، حروب المعلومات 2004م .
http://arabinfo.blogspot.com/2004/08/blog-post_17.html
- 156 - مقاله بعنوان حرب المعلومات على العنوان :
<http://www.alyaseer.net/vb/showthread.php?t=7614>





- 157 - محمد بن سعود الخطيب، حرب المعلومات مصطلح مصري لبدأ أرلي
&http://www.siironline.org/alabwab/maqalat
mohaderat(12)/1202.htm
- 158 - مقالة بعنوان أسلحة حرب المعلومات واستخداماتها على العنوان.
http://yomgedid.kenanaonline.com/topics/56836/posts/94428
- 159 - هشام سليمان، حرب المعلومات الوجه الجديد للحروب 2001
&http://www.islamonline.net/servlet/Satellite?c=ArticleA_C
pagename=Zone-Arabic-
.cid=1175947754312&HealthScience/HSALayout
- 160 - مقالة عن فيروسات الحاسوب على العنوان
/http://ar.wikipedia.org/wiki
- 161 - مقالة عن دودة الحاسوب على العنوان
./http://ar.wikipedia.org/wiki
- 162 - علي بن ضبيان الرشيد، العدوان على البيئة المعلوماتية خطورته ومواجهته، مجلة
كلية الملك خالد العسكرية العدد 81، 01-06-2005م.
&http://www.kkmaq.gov.sa/Detail.asp?InSectionID=1689
.InNewsItemID=164260
- 163 - شبكة النبا المعلوماتية - الخميس 23/حزيران/2011 - 20/رجب/1432.
- 164 - عمر الحياني عضو الرابطة العربية للإعلاميين العلميين اليمن - صنعاء،
http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/51-
forensic-and-computer-crimes/747-war-programs.html
- 165 - محمد عثمان - دبي السبت 28 إبريل 2012 الساعة 02:53
http://alroya.com/node/192881
- 166 - ربطة المرأة العراقية، القرصنة الإلكترونية في العراق: إبتزاز وتدمير مواقع
حكومية، الخميس 23-02-2012 11:58 صباحا
http://iraqiwomensleague.com/news_view_11088.htm
- 167 - هاكرز يخترقون أكبر شركة نفط سعودية، سكاي نيوز، أبو طلي 09
سبتمبر 2012 :-
http://www.skynewsarabia.com/web/article/
http://www.alriyadh.com/2012/10/06/article774008.html - 168
- 169 - المساء يومية اخبارية وطنية دار الصحافة عبدالقادر سفير القبة



الجزائر العاصمة . 2009/12/12 انظر : -

<http://www.el-massa.com/ar/content/view/27763>

<http://www.bokra.net/Articles> - 170

<http://www.dw.de> - 171

172 - - جريدة الشرق الاوسط . الاربعاء 01 رجب 1422 هـ 19 سبتمبر 2001

العدد 8331

<http://www.aawsat.com/details.asp?section=6&article=57933&issue>
no=8331



القرصنة الإلكترونية

أسلحة الحرب الحديثة



دار أسامة
للنشر والتوزيع

الأردن - عمان

هاتف: 00962 6 5658252 / 00962 6 5658253

فاكس: 00962 6 5658254 ص.ب: 141781

البريد الإلكتروني: darasama@orange.jo

الموقع الإلكتروني: www.darasama.net



نيسالا
ناشرون وموزعون

الأردن - عمان - العبدلي

تليفاكس: 0096265664085



ISBN 978-9957-22-550-8



9 789957 225506